PATENT COOPERATION TREATY

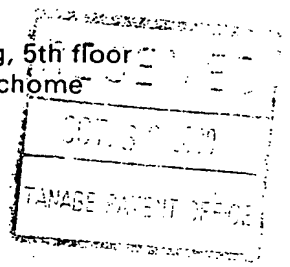
From the INTERNATIONAL BUREAU

PCT

NOTICE INFORMING THE APPLICANT OF THE COMMUNICATION OF THE INTERNATIONAL APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

To:
TANABE, Shigemoto
Green-Fantasia Building, 5th floor
11-11-508, Jingumae 1-chome
Shibuya-ku
Tokyo 150-0001
JAPON



Date of mailing (day/month/year) 19 October 2000 (19.10.00)	
Applicant's or agent's file reference S00P0778WO00	**IMPORTANT NOTICE**

International application No.	**International filing date** (day/month/year)	**Priority date** (day/month/year)
PCT/JP00/02289	07 April 2000 (07.04.00)	12 April 1999 (12.04.99)

Applicant
SONY CORPORATION et al

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:
   KR,US

   In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:
   CN,EP,SG

   The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on
   19 October 2000 (19.10.00) under No. WO 00/62216.

REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, **a demand for international preliminary examination** must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the **national phase**, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer J. Zahra
Facsimile No. (41-22) 740.14.35	Telephone No. (41-22) 338.83.38

Attorney Docket No. 450108-02550

New Patent Application filed **December 8, 2000**, entitled:

INFORMATION PROCESSING APPARATUS, INFORMATION PROCESSING METHOD, AND PROVIDING MEDIUM

corresponding to PCT Application No. PCT/JP00/02289

filed April 7, 2000

Express Mail No.: EL585030619US

Date of Deposit: December 8, 2000

I hereby certify that this application and the accompanying papers are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to:

Box PCT
Assistant Commissioner for Patents
Washington, D.C. 20231.

特　許　協　力　条　約

発信人　日本国特許庁（国際調査機関）

出願人代理人

田辺　恵基　殿

田辺特許 12.6.14 受領

あて名

〒１５０－０００１

東京都渋谷区神宮前１丁目１１番１１－５０８号
グリーンフアンタジアビル５階
田辺特許事務所

S746WO

PCT

国際調査報告又は国際調査報告を作成しない旨の決定の送付の通知書

（法施行規則第４１条）
〔ＰＣＴ規則44.1〕

出願人又は代理人の書類記号　S00P0778WO00	発送日（日.月.年）13.06.00 今後の手続きについては、下記１及び４を参照。
国際出願番号　PCT／JP00／02289	国際出願日（日.月.年）07.04.00
出願人（氏名又は名称）　ソニー株式会社	

1．[X] 国際調査報告が作成されたこと、及びこの送付書とともに送付することを、出願人に通知する。
ＰＣＴ１９条の規定に基づく補正書及び説明書の提出
出願人は、国際出願の請求の範囲を補正することができる（ＰＣＴ規則４６参照）。
いつ　補正書の提出期間は、通常国際調査報告の送付の日から２月である。
詳細については添付用紙の備考を参照すること。
どこへ　直接次の場所へ
The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland
Facsimile No.: (41-22)740.14.35
詳細な手続については、添付用紙の備考を参照すること。

2．[ ] 国際調査報告が作成されないこと、及び法第８条第２項（ＰＣＴ１７条(2)(a)）の規定による国際調査報告を作成しない旨の決定をこの送付書とともに送付することを、出願人に通知する。

3．[ ] 法施行規則第４４条（ＰＣＴ規則40.2）に規定する追加手数料の納付に対する異議の申立てに関して、出願人に下記の点を通知する。
[ ] 異議の申立てと当該異議についての決定を、その異議の申し立てと当該異議についての決定の両方を指定官庁へ送付することを求める出願人の請求とともに、国際事務局へ送付した。
[ ] 当該異議についての決定は、まだ行われていない。決定されしだい出願人に通知する。

4．今後の手続：　出願人は次の点に注意すること。
優先日から１８月経過後、国際出願は国際事務局によりすみやかに国際公開される。出願人が公開の延期を望むときは、国際出願又は優先権の主張の取下げの通知がＰＣＴ規則90の2.1及び90の2.3にそれぞれ規定されているように、国際公開の事務的な準備が完了する前に国際事務局に到達しなければならない。
出願人が優先日から３０月まで（官庁によってはもっと遅く）国内段階の開始を延期することを望むときは、優先日から１９月以内に、国際予備審査の請求書が提出されなければならない。
国際予備審査の請求書若しくは、後にする選択により優先日から１９箇月以内に選択しなかった又は第Ⅱ章に拘束されないため選択できなかったすべての指定官庁に対しては優先日から２０月以内に、国内段階の開始のための所定手続を取らなければならない。

名称及びあて名 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	権限のある職員　５Ｌ　９２８７ 特　許　庁　長　官 電話番号　０３－３５８１－１１０１　内線　３５６２

様式ＰＣＴ／ＩＳＡ／２２０（１９９８年７月）　（添付用紙を参照）

注　　意

1．国際調査報告の発送日から起算する条約第１９条（１）及び規則４６．１に従う国際事務局への補正期間に注意してください。

2．条約２２条（２）に規定する期間に注意してください。

3．文献の写しの請求について

国際調査報告に記載した文献の複写

特許庁にこれらの引用文献の写しを請求することもできますが、日本特許情報機構でもこれらの引用文献の複写物を販売しています。日本特許情報機構に引用文献の複写物を請求する場合は下記の点に注意してください。

〔申込方法〕

（１）特許（実用新案・意匠）公報については、下記の点を明記してください。

○特許・実用新案及び意匠の種類

○出願公告又は出願公開の年次及び番号（又は特許番号、登録番号）

○必要部数

（２）公報以外の文献の場合は、下記の点に注意してください。

○国際調査報告の写しを添付してください（返却します）。

〔申込み及び照会先〕

〒１３５　東京都江東区東陽４－１－７　佐藤ダイヤビル

財団法人　日本特許情報機構　サービス課

ＴＥＬ　０３－５６９０－３９００

注意　　特許庁に対して文献の写しの請求をすることができる期間は、国際出願日から７年です。

様式ＰＣＴ／ＩＳＡ／２２０の備考

この備考は、ＰＣＴ１９条の規定に基づく補正書の提出に関する基本的な指示を与えるためのものである。この備考は特許協力条約並びにこの条約に基づく規則及び実施細則の規定に基づいている。この備考とそれらの規定とが相違する場合には、後者が適用される。詳細な情報については、ＷＩＰＯの出版物であるＰＣＴ出願人の手引も参照すること。

ＰＣＴ１９条の規定に基づく補正書の提出に関する指示

出願人は、国際調査報告を受領した後、国際出願の請求の範囲を補正する機会が一回ある。しかし、国際出願のすべての部分（請求の範囲、明細書及び図面）が、国際予備審査の手続においても補正できるもので、例えば出願人が仮保護のために補正書を公開することを希望する場合又は国際公開前に請求の範囲を補正する別の理由がある場合を除き、通常ＰＣＴ１９条の規定に基づく補正書を提出する必要はないことを強調しておく。さらに、仮保護は一部の国のみで与えられるだけであることも強調しておく。

補正の対象となるもの

ＰＣＴ１９条の規定により請求の範囲のみ補正することができる。
国際段階においてＰＣＴ３４条の規定に基づく国際予備審査の手続きにおいて請求の範囲を（更に）補正することができる。
明細書及び図面は、ＰＣＴ３４条の規定に基づく国際予備審査の手続においてのみ補正することができる。
国内段階に移行する際、ＰＣＴ２８条（又はＰＣＴ４１条）の規定により、国際出願のすべての部分を補正することができる。

いつ

国際調査報告の送付の日から２月又は優先日から１６月の内どちらか遅く満了するほうの期間内。しかし、その期間の満了後であっても国際公開の技術的な準備の完了前に国際事務局が補正を受領した場合には、その補正書は、期間内に受理されたものとみなすことを強調しておく（ＰＣＴ規則46.1）。

補正書を提出すべきところ

補正書は、国際事務局のみに提出でき、受理官庁又は国際調査機関には提出してはいけない（ＰＣＴ規則46.2）。
国際予備審査の請求書を提出した／する場合については、以下を参照すること。

どのように

１以上の請求の範囲の削除、１以上の新たな請求の範囲の追加、又は１以上の請求の範囲の記載の補正による。
差替え用紙は、補正の結果、出願当初の用紙と相違する請求の範囲の各用紙毎に提出する。
差替え用紙に記載されているすべての請求の範囲には、アラビア数字を付さなければならない。請求の範囲を削除する場合、その他の請求の範囲の番号を付け直す必要はない。請求の範囲の番号を付け直す場合には、連続番号で付け直さなければならない（ＰＣＴ実施細則第205号(b)）。
補正は国際公開の言語で行う。

補正書にどのような書類を添付しなければならないか

書簡（ＰＣＴ実施細則第205号(b)）

補正書には書簡を添付しなければならない。
書簡は国際出願及び補正された請求の範囲とともに公開されることはない。これを「ＰＣＴ１９条(1)に規定する説明書」と混同してはならない（「ＰＣＴ１９条(1)に規定する説明書」については、以下を参照）。
書簡は、英語又は仏語を選択しなければならない。ただし、国際出願の言語が英語の場合、書簡は英語で、仏語の場合、書簡は仏語で記載しなければならない。
書簡には、出願時の請求の範囲と補正された請求の範囲との相違について表示しなければならない。特に、国際出願に記載した各請求の範囲との関連で次の表示（２以上の請求の範囲についての同一の表示する場合は、まとめることができる。）をしなければならない。
(i) この請求の範囲は変更しない。
(ii) この請求の範囲は削除する。
(iii) この請求の範囲は追加である。
(iv) この請求の範囲は出願時の１以上の請求の範囲と差し替える。
(v) この請求の範囲は出願時の請求の範囲の分割の結果である。

様式ＰＣＴ／ＩＳＡ／２２０の備考（続き）

次に、添付する書簡中での、補正についての説明の例を示す。

１．［請求の範囲の一部の補正によって請求の範囲の項数が４８から５１になった場合］：
“請求の範囲１－２９、３１、３２、３４、３５、３７－４８項は、同じ番号のもとに補正された請求の範囲と置き換えられた。請求の範囲３０、３３及び３６項は変更なし。新たに請求の範囲４９－５１項が追加された。”
２．［請求の範囲の全部の補正によって請求の範囲の項数が１５から１１になった場合］：
“請求の範囲１－１５項は、補正された請求の範囲１－１１項に置き換えられた。”
３．［原請求の範囲の項数が１４で、補正が一部の請求の範囲の削除と新たな請求の範囲の追加を含む場合］：
“請求の範囲１－６及び１４項は変更なし。請求の範囲７－１３は削除。新たに請求の範囲１５、１６及び１７項を追加。”又は
“請求の範囲７－１３は削除。新たに請求の範囲１５、１６及び１７項を追加。その他の全ての請求の範囲は変更なし。”
４．［各種の補正がある場合］：
“請求の範囲１－１０項は変更なし。請求の範囲１１－１３、１８及び１９項は削除。請求の範囲１４、１５及び１６項は補正された請求の範囲１４項に置き換えられた。請求の範囲１７項は補正された請求の範囲１５、１６及び１７項に分割された。新たに請求の範囲２０及び２１項が追加された。”

“ＰＣＴ１９条(1)の規定に基づく説明書”（ＰＣＴ規則46.4）

補正書には、補正並びにその補正が明細書及び図面に与える影響についての説明書を提出することができる（明細書及び図面はＰＣＴ１９条(1)の規定に基づいては補正できない）。

説明書は、国際出願及び補正された請求の範囲とともに公開される。

説明書は、国際公開の言語で作成しなければならない。

説明書は、簡潔でなければならず、英語の場合又は英語に翻訳した場合に５００語を越えてはならない。

説明書は、出願時の請求の範囲と補正された請求の範囲との相違を示す書簡と混同してはならない。説明書を、その書簡に代えることはできない。説明書は別紙で提出しなければならず、見出しを付すものとし、その見出しは“ＰＣＴ１９条(1)の規定に基づく説明書”の語句を用いることが望ましい。

説明書には、国際調査報告又は国際調査報告に列記された文献との関連性に関して、これらを誹謗する意見を記載してはならない。国際調査報告に列記された特定の請求の範囲に関連する文献についての言及は、当該請求の範囲の補正に関してのみ行うことができる。

国際予備審査の請求書が提出されている場合

ＰＣＴ１９条の規定に基づく補正書及び添付する説明書の提出の時に国際予備審査の請求書が既に提出されている場合には、出願人は、補正書（及び説明書）を国際事務局に提出すると同時にその写し及び必要な場合、その翻訳文を国際予備審査機関にも提出することが望ましい（ＰＣＴ規則55.3(a)、62.2の第１文を参照）。詳細は国際予備審査請求書（ＰＣＴ／ＩＰＥＡ／４０１）の注意書参照。

国内段階に移行するための国際出願の翻訳に関して

国内段階に移行する際、ＰＣＴ１９条の規定に基づいて補正された請求の範囲の翻訳を出願時の請求の範囲の翻訳の代わりに又は追加して、指定官庁／選択官庁に提出しなければならないこともあるので、出願人は注意されたい。

指定官庁／選択官庁の詳細な要求については、ＰＣＴ出願人の手引きの第Ⅱ巻を参照。

特　許　協　力　条　約

PCT

国際調査報告

（法８条、法施行規則第40、41条）
〔ＰＣＴ１８条、ＰＣＴ規則43、44〕

出願人又は代理人の書類記号　S00P0778WO00	今後の手続きについては、国際調査報告の送付通知様式（ＰＣＴ／ＩＳＡ／２２０）及び下記５を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ００／０２２８９	国際出願日 (日.月.年)　０７．０４．００	優先日 (日.月.年)　１２．０４．９９
出願人（氏名又は名称） ソニー株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条（ＰＣＴ１８条）の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で　2　ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

１．国際調査報告の基礎

ａ．言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

ｂ．この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際調査機関に提出された書面による配列表
☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

２．☐ 請求の範囲の一部の調査ができない（第Ⅰ欄参照）。

３．☐ 発明の単一性が欠如している（第Ⅱ欄参照）。

４．発明の名称は
☒ 出願人が提出したものを承認する。
☐ 次に示すように国際調査機関が作成した。

５．要約は
☒ 出願人が提出したものを承認する。
☐ 第Ⅲ欄に示されているように、法施行規則第47条（ＰＣＴ規則38.2(b)）の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から１カ月以内にこの国際調査機関に意見を提出することができる。

６．要約書とともに公表される図は、
第　２０　図とする。☒ 出願人が示したとおりである。　☐ なし
☐ 出願人は図を示さなかった。
☐ 本図は発明の特徴を一層よく表している。

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／０２２８９

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int. Cl' G06F17/60

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int. Cl' G06F17/60 G06F13/00 G09C1/00 H04L9/08 G06F15/00 H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　1926-1996年
日本国公開実用新案公報　1971-2000年
日本国実用新案登録公報　1996-2000年
日本国登録実用新案公報　1994-2000年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JICSTデータベース(JOIS)

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	WO,96/27155,A2(InerTrust Technologies Corp.),6.9月.1996(06.09.96&JP,10-512074,A	1-9
A	US,6002771,A(Sun Microsystems, Incorporated)22.5月.96(22.05.96)&JP,10-055383,A	1-9

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
24.05.00	13.06.00

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	岩間　直純	5L	9287
	電話番号　０３－３５８１－１１０１　内線　3532		

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

控

特許協力条約に基づく[redacted]際出願

願　　書

出願人は、この国際出願が特許協力条約に従って処理されることを請求する。

国際事務局記入欄	
国際出願番号	[redacted]
国際出願日	PCT 07.4.00 受領印
(受付印)	

出願人又は代理人の書類記号 (希望する場合、最大12字)	S00P0778WO00

PTO/PCT Rec'd 08 DEC 2000

第I欄　発明の名称

情報処理装置および方法、並びに提供媒体

第II欄　出願人

氏名（名称）及びあて名：（姓・名の順に記載；法人は公式の完全な名称を記載；あて名は郵便番号及び国名も記載）

ソニー株式会社
SONY CORPORATION
〒141-0001 日本国東京都品川区北品川6丁目7番35号
7-35, Kitashinagawa 6-chome, Shinagawa-ku, TOKYO 141-0001, JAPAN

☐ この欄に記載した者は、発明者でもある。

電話番号：03-5448-2617
ファクシミリ番号：03-5448-3063
加入電信番号：J22262

国籍（国名）：日本国　JAPAN
住所（国名）：日本国　JAPAN

この欄に記載した者は、次の指定国についての出願人である：
☐ すべての指定国　☑ 米国を除くすべての指定国　☐ 米国のみ　☐ 追記欄に記載した指定国

第III欄　その他の出願人又は発明者

氏名（名称）及びあて名：（姓・名の順に記載；法人は公式の完全な名称を記載；あて名は郵便番号及び国名も記載）

石橋　義人　　ISHIBASHI Yoshihito
〒141-0001 日本国東京都品川区北品川6丁目7番35号
ソニー株式会社内
C/O SONY CORPORATION, 7-35, Kitashinagawa 6-chome, Shinagawa-ku, TOKYO 141-0001, JAPAN

この欄に記載した者は次に該当する：
☐ 出願人のみである。
☑ 出願人及び発明者である。
☐ 発明者のみである。（ここにレ印を付したときは、以下に記入しないこと）

国籍（国名）：日本国　JAPAN
住所（国名）：日本国　JAPAN

この欄に記載した者は、次の指定国についての出願人である：
☐ すべての指定国　☐ 米国を除くすべての指定国　☑ 米国のみ　☐ 追記欄に記載した指定国

☑ その他の出願人又は発明者が続葉に記載されている。

第IV欄　代理人又は共通の代表者、通知のあて名

次に記載された者は、国際機関において出願人のために行動する：☑ 代理人　☐ 共通の代表者

氏名（名称）及びあて名：（姓・名の順に記載；法人は公式の完全な名称を記載；あて名は郵便番号及び国名も記載）

8274　弁理士　田　辺　恵　基　　TANABE Shigemoto
〒150-0001 日本国東京都渋谷区神宮前1丁目11番11-508号
グリーンファンタジアビル5階
Green-Fantasia Building 5th Floor, 11-11-508, Jingumae 1-chome, Shibuya-ku, TOKYO 150-0001, JAPAN

電話番号：03-3470-6591
ファクシミリ番号：03-3470-6506
加入電信番号：

☐ 通知のためのあて名：代理人又は共通の代表者が選任されておらず、上記枠内に特に通知が送付されるあて名を記載している場合は、レ印を付す。

第Ⅲ欄の続き　その他の[redacted]願人又は発明者

この続葉を使用しないときは、この用紙を願書に含めないこと。

氏名（名称）及びあて名：*（姓・名の順に記載；法人は公式の完全な名称を記載；あて名は郵便番号及び国名も記載）*

大石　丈於　　OHISHI Tateo
〒141-0001 日本国東京都品川区北品川６丁目７番３５号
ソニー株式会社内
C/O SONY CORPORATION, 7-35, Kitashinagawa 6-chome,
Shinagawa-ku, TOKYO 141-0001, JAPAN

この欄に記載した者は、次に該当する：
☐ 出願人のみである。
☑ 出願人及び発明者である。
☐ 発明者のみである。
（ここにレ印を付したときは、以下に記入しないこと）

国籍 *（国名）*：日本国　JAPAN
住所 *（国名）*：日本国　JAPAN

この欄に記載した者は、次の指定国についての出願人である：
☐ すべての指定国　☐ 米国を除くすべての指定国　☑ 米国のみ　☐ 追記欄に記載した指定国

氏名（名称）及びあて名：*（姓・名の順に記載；法人は公式の完全な名称を記載；あて名は郵便番号及び国名も記載）*

武藤　明宏　　MUTO Akihiro
〒141-0001 日本国東京都品川区北品川６丁目７番３５号
ソニー株式会社内
C/O SONY CORPORATION, 7-35, Kitashinagawa 6-chome,
Shinagawa-ku, TOKYO 141-0001, JAPAN

この欄に記載した者は、次に該当する：
☐ 出願人のみである。
☑ 出願人及び発明者である。
☐ 発明者のみである。
（ここにレ印を付したときは、以下に記入しないこと）

国籍 *（国名）*：日本国　JAPAN
住所 *（国名）*：日本国　JAPAN

この欄に記載した者は、次の指定国についての出願人である：
☐ すべての指定国　☐ 米国を除くすべての指定国　☑ 米国のみ　☐ 追記欄に記載した指定国

氏名（名称）及びあて名：*（姓・名の順に記載；法人は公式の完全な名称を記載；あて名は郵便番号及び国名も記載）*

この欄に記載した者は、次に該当する：
☐ 出願人のみである。
☐ 出願人及び発明者である。
☐ 発明者のみである。
（ここにレ印を付したときは、以下に記入しないこと）

国籍 *（国名）*：
住所 *（国名）*：

この欄に記載した者は、次の指定国についての出願人である：
☐ すべての指定国　☐ 米国を除くすべての指定国　☐ 米国のみ　☐ 追記欄に記載した指定国

氏名（名称）及びあて名：*（姓・名の順に記載；法人は公式の完全な名称を記載；あて名は郵便番号及び国名も記載）*

この欄に記載した者は、次に該当する：
☐ 出願人のみである。
☐ 出願人及び発明者である。
☐ 発明者のみである。
（ここにレ印を付したときは、以下に記入しないこと）

国籍 *（国名）*：
住所 *（国名）*：

この欄に記載した者は、次の指定国についての出願人である：
☐ すべての指定国　☐ 米国を除くすべての指定国　☐ 米国のみ　☐ 追記欄に記載した指定国

☐ その他の出願人又は発明者が他の続葉に記載されている。

第Ⅴ欄　国の指定

規則 4.9(a)の規定に基づき次の指定を行う（該当する□にレ印を付すこと；　少なくとも1つの□にレ印を付すこと）。

広域特許

☐ ＡＰ　ＡＲＩＰＯ特許：ＧＨ ガーナ Ghana, ＧＭ ガンビア Gambia, ＫＥ ケニア Kenya, ＬＳ レソト Lesotho, ＭＷ マラウイ Malawi, ＳＤ スーダン Sudan, ＳＬ シエラ・レオーネ Sierra Leone, ＳＺ スワジランド Swaziland, ＴＺ タンザニア United Republic of Tanzania, ＵＧ ウガンダ Uganda, ＺＷ ジンバブエ Zimbabwe, 及びハラレプロトコルと特許協力条約の締約国である他の国

☐ ＥＡ　ユーラシア特許：ＡＭ アルメニア Armenia, ＡＺ アゼルバイジャン Azerbaijan, ＢＹ ベラルーシ Belarus, ＫＧ キルギス Kyrgyzstan, ＫＺ カザフスタン Kazakhstan, ＭＤ モルドヴァ Republic of Moldova, ＲＵ ロシア Russian Federation, ＴＪ タジキスタン Tajikistan, ＴＭ トルクメニスタン Turkmenistan, 及びユーラシア特許条約と特許協力条約の締約国である他の国

☑ ＥＰ　ヨーロッパ特許：~~ＡＴ オーストリア Austria, ＢＥ ベルギー Belgium, ＣＨ and ＬＩ スイス及びリヒテンシュタイン Switzerland and Liechtenstein, ＣＹ キプロス Cyprus,~~ ＤＥ ドイツ Germany, ~~ＤＫ デンマーク Denmark, ＥＳ スペイン Spain, ＦＩ フィンランド Finland,~~ ＦＲ フランス France, ＧＢ 英国 United Kingdom, ~~ＧＲ ギリシャ Greece, ＩＥ アイルランド Ireland, ＩＴ イタリア Italy, ＬＵ ルクセンブルグ Luxembourg, ＭＣ モナコ Monaco, ＮＬ オランダ Netherlands, ＰＴ ポルトガル Portugal, ＳＥ スウェーデン Sweden,~~ 及びヨーロッパ特許条約と特許協力条約の締約国である他の国

☐ ＯＡ　ＯＡＰＩ特許：ＢＦ ブルキナ・ファソ Burkina Faso, ＢＪ ベナン Benin, ＣＦ 中央アフリカ Central African Republic, ＣＧ コンゴー Congo, ＣＩ コートジボアール Côte d'Ivoire, ＣＭ カメルーン Cameroon, ＧＡ ガボン Gabon, ＧＮ ギニア Guinea, ＧＷ ギニア・ビサオ Guinea-Bissau, ＭＬ マリ Mali, ＭＲ モーリタニア Mauritania, ＮＥ ニジェール Niger, ＳＮ セネガル Senegal, ＴＤ チャード Chad, ＴＧ トーゴー Togo, 及びアフリカ知的所有権機構のメンバー国と特許協力条約の締約国である他の国 *(他の種類の保護又は取扱いを求める場合には点線上に記載する)* .....

国内特許 *(他の種類の保護又は取扱いを求める場合には点線上に記載する)*

☐ ＡＥ アラブ首長国連邦 United Arab Emirates
☐ ＡＬ アルバニア Albania .....
☐ ＡＭ アルメニア Armenia .....
☐ ＡＴ オーストリア Austria .....
☐ ＡＵ オーストラリア Australia .....
☐ ＡＺ アゼルバイジャン Azerbaijan
☐ ＢＡ ボスニア・ヘルツェゴヴィナ Bosnia and Herzegovina
.....
☐ ＢＢ バルバドス Barbados
☐ ＢＧ ブルガリア Bulgaria .....
☐ ＢＲ ブラジル Brazil .....
☐ ＢＹ ベラルーシ Belarus .....
☐ ＣＡ カナダ Canada
☐ ＣＨ and ＬＩ スイス及びリヒテンシュタイン Switzerland and Liechtenstein
☑ ＣＮ 中国 China .....
☐ ＣＲ コスタリカ Costa Rica .....
☐ ＣＵ キューバ Cuba .....
☐ ＣＺ チェッコ Czech Republic .....
☐ ＤＥ ドイツ Germany .....
☐ ＤＫ デンマーク Denmark .....
☐ ＤＭ ドミニカ Dominica
☐ ＥＥ エストニア Estonia .....
☐ ＥＳ スペイン Spain .....
☐ ＦＩ フィンランド Finland .....
☐ ＧＢ 英国 United Kingdom
☐ ＧＤ グレナダ Grenada
☐ ＧＥ グルジア Georgia .....
☐ ＧＨ ガーナ Ghana .....
☐ ＧＭ ガンビア Gambia
☐ ＨＲ クロアチア Croatia .....
☐ ＨＵ ハンガリー Hungary .....
☐ ＩＤ インドネシア Indonesia
☐ ＩＬ イスラエル Israel .....
☐ ＩＮ インド India .....
☐ ＩＳ アイスランド Iceland
☐ ＪＰ 日本 Japan .....
☐ ＫＥ ケニア Kenya .....
☐ ＫＧ キルギス Kyrgyzstan .....
☐ ＫＰ 北朝鮮 Democratic People's Republic of Korea .....
☑ ＫＲ 韓国 Republic of Korea .....
☐ ＫＺ カザフスタン Kazakhstan .....
☐ ＬＣ セント・ルシア Saint Lucia
☐ ＬＫ スリ・ランカ Sri Lanka
☐ ＬＲ リベリア Liberia
☐ ＬＳ レソト Lesotho .....
☐ ＬＴ リトアニア Lithuania
☐ ＬＵ ルクセンブルグ Luxembourg
☐ ＬＶ ラトヴィア Latvia
☐ ＭＡ モロッコ Morocco .....
☐ ＭＤ モルドヴァ Republic of Moldova .....
☐ ＭＧ マダガスカル Madagascar .....
☐ ＭＫ マケドニア旧ユーゴースラヴィア共和国 The former Yugoslav Republic of Macedonia .....
☐ ＭＮ モンゴル Mongolia
☐ ＭＷ マラウイ Malawi .....
☐ ＭＸ メキシコ Mexico .....
☐ ＮＯ ノールウェー Norway
☐ ＮＺ ニュー・ジーランド New Zealand .....
☐ ＰＬ ポーランド Poland .....
☐ ＰＴ ポルトガル Portugal .....
☐ ＲＯ ルーマニア Romania
☐ ＲＵ ロシア Russian Federation .....
☐ ＳＤ スーダン Sudan
☐ ＳＥ スウェーデン Sweden
☑ ＳＧ シンガポール Singapore
☐ ＳＩ スロヴェニア Slovenia .....
☐ ＳＫ スロヴァキア Slovakia .....
☐ ＳＬ シエラ・レオーネ Sierra Leone .....
☐ ＴＪ タジキスタン Tajikistan .....
☐ ＴＭ トルクメニスタン Turkmenistan .....
☐ ＴＲ トルコ Turkey .....
☐ ＴＴ トリニダッド・トバゴ Trinidad and Tobago .....
☐ ＴＺ タンザニア United Republic of Tanzania
☐ ＵＡ ウクライナ Ukraine .....
☐ ＵＧ ウガンダ Uganda .....
☑ ＵＳ 米国 United States of America .....
.....
☐ ＵＺ ウズベキスタン Uzbekistan .....
☐ ＶＮ ヴィエトナム Viet Nam .....
☐ ＹＵ ユーゴースラヴィア Yugoslavia .....
☐ ＺＡ 南アフリカ共和国 South Africa .....
☐ ＺＷ ジンバブエ Zimbabwe .....

下の□は、この様式の施行後に特許協力条約の締約国となった国を指定するためのものである

☐ .....
☐ .....
☐ .....

指定の確認の宣言：出願人は、上記の指定に加えて、規則 4.9(b)の規定に基づき、特許協力条約の下で認められる他の全ての国の指定を行う。ただし、この宣言書から除く旨の表示を追記欄にした国は、指定から除かれる。出願人は、これらの追加される指定が確認を条件としていること、並びに優先日から15月が経過する前にその確認がなされない指定は、この期間の経過時に、出願人によって取り下げられたものとみなされることを宣言する。*(指定の確認(料金を含む)は、優先日から15月以内に受理官庁へ提出しなければならない。)*

第VI欄　優先権主張

☐ 他の優先権の主張（先の出願）が追記欄に記載されている

先の出願日 (日. 月. 年)	先の出願番号	先の出願		
		国内出願：国名	広域出願：＊広域官庁名	国際出願：受理官庁名
(1) 12.04.99	平成１１年特許願 第１０３９９３号	日本国　JAPAN		
(2)				
(3)				

☐ 上記（ ）の番号の先の出願（ただし、本国際出願が提出される受理官庁に対して提出されたものに限る）のうち、次の（ ）の番号のものについては、出願書類の認証謄本を作成し国際事務局へ送付することを、受理官庁（日本国特許庁の長官）に対して請求している。　：

＊先の出願が、ＡＲＩＰＯの特許出願である場合には、その先の出願を行った工業所有権の保護のためのパリ条約同盟国の少なくとも１ヶ国を追記欄に表示しなければならない（規則４．１０(b)(ii)）。追記欄を参照。

第VII欄　国際調査機関

国際調査機関（ＩＳＡ）の選択

ＩＳＡ／ＪＰ

先の調査結果の利用請求：当該調査の照会（先の調査が、国際調査機関によって既に実施又は請求されている場合）

出願日（日. 月. 年）　出願番号　国名（又は広域官庁）

第VIII欄　照合欄：出願の言語

この国際出願の用紙の枚数は次のとおりである。

願書	4 枚
明細書（配列表を除く）	62 枚
請求の範囲	5 枚
要約書	1 枚
図面	50 枚
明細書の配列表	0 枚
合計	122 枚

この国際出願には、以下にチェックした書類が添付されている。

1. ☑ 手数料計算用紙
   ☑ 納付する手数料に相当する特許印紙を貼付した書面
   ☑ 国際事務局の口座への振込みを証明する書面
2. ☐ 別個の記名押印された委任状
3. ☐ 包括委任状の写し
4. ☐ 記名押印（署名）の説明書
5. ☐ 優先権書類（上記第VI欄の（ ）の番号を記載する）：
6. ☐ 国際出願の翻訳文（翻訳に使用した言語名を記載する）：
7. ☐ 寄託した微生物又は他の生物材料に関する書面
8. ☐ ヌクレオチド又はアミノ酸配列表（フレキシブルディスク）
9. ☐ その他（書類名を詳細に記載する）：

要約書とともに提示する図面：　20

本国際出願の使用言語名：　日本語

第IX欄　提出者の記名押印

各人の氏名（名称）を記載し、その次に押印する。

田　辺　恵　基

受理官庁記入欄

1. 国際出願として提出された書類の実際の受理の日

3. 国際出願として提出された書類を補完する書類又は図面であって
   その後期間内に提出されたものの実際の受理の日（訂正日）

4. 特許協力条約第１１条(2)に基づく必要な補完の期間内の受理の日

5. 出願人により特定された国際調査機関　ＩＳＡ／ＪＰ

6. ☐ 調査手数料未払いにつき、国際調査機関に調査用写しを送付していない

2. 図面
   ☐ 受理された
   ☐ 不足図面がある

国際事務局記入欄

記録原本の受理の日

この用紙は、国際出願の一部を構成せず、国際出願の用紙の枚数に算入しない。

PCT

手数料計算用紙

願書附属書

受理官庁記入欄

国際出願番号

受理官庁の日付印

出願人又は代理人の書類記号

S00P0778WO00

出願人

ソニー株式会社　SONY CORPORATION

所定の手数料の計算

1．及び2．特許協力条約に基づく国際出願等に関する法律（国内法）第18条第1項第1号の規定による手数料 *(注1)*
（送付手数料〔T〕及び調査手数料〔S〕の合計）　95,000 円　T+S

3．国際手数料 *(注2)*

基本手数料

国際出願に含まれる用紙の枚数　122 枚

最初の30枚まで　46,000 円　b1

92（30枚を超える用紙の枚数）× 1,100（用紙1枚の手数料）= 101,200 円　b2

b1及びb2に記入した金額を加算し、合計額をBに記入　147,200 円　B

指定手数料

国際出願に含まれる指定数 *(注3)*　5

5（支払うべき指定手数料の数 *(上限は8)* *(注4)*）× 9,900（1指定当たりの手数料）= 49,500 円　D

B及びDに記入した金額を加算し、合計額をIに記入　196,700 円　I

4．納付すべき手数料の合計

T+S及びIに記入した金額を加算し、合計額を合計に記入　291,700 円

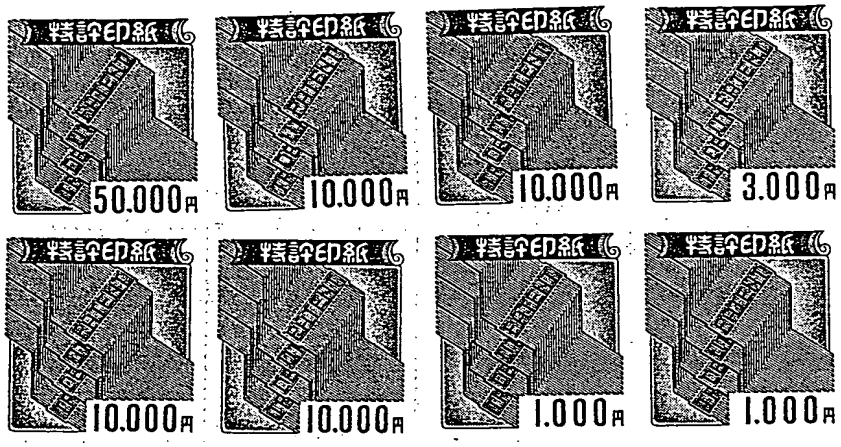
合　計

(注1) 送付手数料及び調査手数料については、合計金額を特許印紙をもって納付しなければならない。

(注2) 国際手数料については、受理官庁である日本国特許庁の長官が告示する国際事務局の口座への振込みを証明する書面を提出することにより納付しなければならない。

(注3) 願書第V欄でレ印を付した□の数。

(注4) 指定数を記入する。　ただし、8指定以上は一律8とする。



送付手数料 (18,000円)
調査手数料 (77,000円)

ご依頼日 年 00 月 04 日 07

振込金(兼消費税等込手数料)受取書

先方銀行

漢字 ⬇ 漢字で左づめでご記入ください: 東京三菱

○印をおつけください。 銀行 ○ 信金 ○ 信組 ○ 農協 ○ 労金 ○ その他 ○

⬇ 漢字で左づめでご記入ください: 内幸町

お受取人

カタカナ(カタカナで姓と名の間はひとマスあけてください): ワイポ゜ヒ゜ィーシィーテ

カタカナ(濁点(゛)と半濁点(゜)も一字でご記入ください): イー

普通預金通帳 ○印をおつけください。 普通 ○ 当座 ○ 貯蓄 ○ その他 ○

口座番号 右づめでご記入ください: 0473286

振込方法 ○印をおつけください。 電信 ○ 文書 ○

金額: ¥196,700 (十億 億 千万 百万 拾万 万 千 百 拾 円)

手数料: ¥735

おなまえ: WIPO - PCT 様

おところ: おでんわ (03)3506-3856

ご依頼人

カタカナ(カタカナで姓と名の間はひとマスあけてください): タナヘ゛ シケ゛モト

カタカナ(濁点(゛)と半濁点(゜)も一字でご記入ください):

(連絡先おでんわ) 市外局番 03 - 市内局番 3470 - 番号 6570

おなまえ: 田辺恵基 様

おところ: 渋谷区神宮前1-11-11-508 グリーンファンタジアビル5階

受取人等はカナ文字で送信しますので、フリガナは正しくていねいにご記入ください。
振込依頼書にご記入相違等の不備がありますと照会等のため振込が遅延することがあります。
午後2時以降のご用命の場合は、当日中に入金できないこともございますので、あらかじめご了承ください。
万一、通信機器・回線等の障害が生じた場合、振込が遅延したことによる補償はできませんのでご了承ください。

当行をご利用くださいましてありがとうございます。
今後ともよろしくお願い申しあげます。

翌日発信扱

当行本支店への振込のために受入れた下記の小切手等が不渡りとなったときは、その金額の振込を取消し、その小切手等は権利保全の手続きをしないで当店において返却します。

未決済小切手等

株式会社 国民銀行
原宿支店

収入印紙
振込金+手数料
3万円以上貼付
17号文書
(払戻請求書による受付書としたものは非課税)

(為104)

基本手数料 (147,200円)
指定手数料 (49,500円)
計 196,700 円

世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類7 G06F 17/60	A1	(11) 国際公開番号	WO00/62216
		(43) 国際公開日	2000年10月19日(19.10.00)

(21) 国際出願番号 PCT/JP00/02289

(22) 国際出願日 2000年4月7日(07.04.00)

(30) 優先権データ
特願平11/103993 1999年4月12日(12.04.99) JP

(71) 出願人（米国を除くすべての指定国について）
ソニー株式会社(SONY CORPORATION)[JP/JP]
〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
石橋義人(ISHIBASHI, Yoshihito)[JP/JP]
大石丈於(OHISHI, Tateo)[JP/JP]
武藤明宏(MUTO, Akihiro)[JP/JP]
〒141-0001 東京都品川区北品川6丁目7番35号
ソニー株式会社内 Tokyo, (JP)
(74) 代理人
弁理士 田辺恵基(TANABE, Shigemoto)
〒150-0001 東京都渋谷区神宮前1丁目11番11-508号
グリーンフアンタジアビル5階 Tokyo, (JP)

(81) 指定国 CN, KR, SG, US, 欧州特許 (DE, FR, GB)

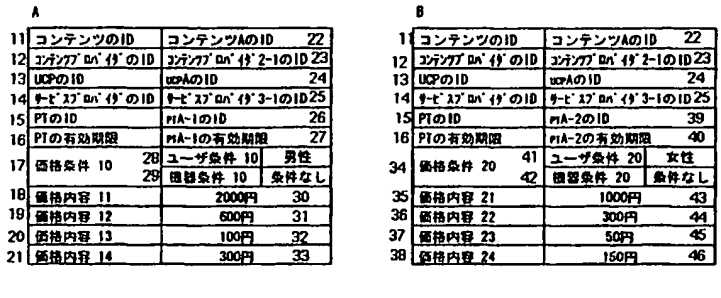
添付公開書類
国際調査報告書

(54)Title: **INFORMATION PROCESSING DEVICE AND METHOD, AND PROVIDING MEDIUM**

(54)発明の名称 情報処理装置および方法、並びに提供媒体

(57) **Abstract**

It is possible to provide service according to user information. PTA-1 can be selected exclusively by a male user because "user condition 10" of "price condition 10" of PTA-1 indicates that the user is a male. PTA-2 can be selected exclusively by a female user because "user condition 20" of "price condition 20" of PTA-2 indicates that the user is a female. The amount of money indicated in the price contents of PTA-2 is half the amount of money of the corresponding PTA-1. In short, a female user can use the contents at a half price, as compared with a male user.



A

11	コンテンツのID		コンテンツAのID	22
12	ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞのID		ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1のID	23
13	UCPのID		UCPAのID	24
14	ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞのID		ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ3-1のID	25
15	PTのID		PTA-1のID	26
16	PTの有効期限		PTA-1の有効期限	27
17	価格条件 10	28	ユーザ条件 10	男性
		29	機器条件 10	条件なし
18	価格内容 11		2000円	30
19	価格内容 12		600円	31
20	価格内容 13		100円	32
21	価格内容 14		300円	33

PTA-1

B

11	コンテンツのID		コンテンツAのID	22
12	ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞのID		ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1のID	23
13	UCPのID		UCPAのID	24
14	ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞのID		ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ3-1のID	25
15	PTのID		PTA-2のID	39
16	PTの有効期限		PTA-2の有効期限	40
34	価格条件 20	41	ユーザ条件 20	女性
		42	機器条件 20	条件なし
35	価格内容 21		1000円	43
36	価格内容 22		300円	44
37	価格内容 23		50円	45
38	価格内容 24		150円	46

PTA-2

A

11...ID OF CONTENTS
12...ID OF CONTENTS PROVIDER
13...ID OF UCP
14...ID OF SERVICE PROVIDER
15...ID OF PT
16...EXPIRATION OF PT
17...PRICE CONDITION 10
18...PRICE CONTENTS 11
19...PRICE CONTENTS 12
20...PRICE CONTENTS 13
21...PRICE CONTENTS 14
22...ID OF CONTENTS A
23...ID OF CONTENTS PROVIDER 2-1
24...ID OF UCPA
25...ID OF SERVICE PROVIDER 3-1
26...ID OF PTA-1
27...EXPIRATION OF PTA-1
28...USER CONDITION 10 MALE
29...DEVICE CONDITION 10 NONE
30...¥2,000
31...¥600
32...¥100
33...¥300

B

34...PRICE CONDITION 20
35...PRICE CONTENTS 21
36...PRICE CONTENTS 22
37...PRICE CONTENTS 23
38...PRICE CONTENTS 24
39...ID OF PTA-2
40...EXPIRATION OF PTA-2
41...USER CONDITION 20 FEMALE
42...DEVICE CONDITION 20 NONE
43...¥1,000
44...¥300
45...¥50
46...¥150

ユーザ情報に応じてサービスを提供できるようにする。

ＰＴＡ－１の「価格条件１０」の「ユーザ条件１０」には、男性のユーザであるとが示されているので、ＰＴＡ－１は、男性のユーザのみが選択可能となる。ＰＴＡ－２の「価格条件２０」の「ユーザ条件２０」には、女性のユーザであることが示されているので、ＰＴＡ－２は、女性のユーザのみが選択可能となる。ＰＴＡ－１とＰＴＡ－２の価格内容を比較すると、ＰＴＡ－２の価格内容に示される額は、対応するＰＴＡ－１の価格内容に示される額の半分にされている。すなわち、女性ユーザは、男性ユーザに比べ、半額の料金でコンテンツを利用することができる。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE	アラブ首長国連邦	DM	ドミニカ	KZ	カザフスタン	RU	ロシア
AG	アンティグア・バーブーダ	DZ	アルジェリア	LC	セントルシア	SD	スーダン
AL	アルバニア	EE	エストニア	LI	リヒテンシュタイン	SE	スウェーデン
AM	アルメニア	ES	スペイン	LK	スリ・ランカ	SG	シンガポール
AT	オーストリア	FI	フィンランド	LR	リベリア	SI	スロヴェニア
AU	オーストラリア	FR	フランス	LS	レソト	SK	スロヴァキア
AZ	アゼルバイジャン	GA	ガボン	LT	リトアニア	SL	シエラ・レオネ
BA	ボズニア・ヘルツェゴビナ	GB	英国	LU	ルクセンブルグ	SN	セネガル
BB	バルバドス	GD	グレナダ	LV	ラトヴィア	SZ	スワジランド
BE	ベルギー	GE	グルジア	MA	モロッコ	TD	チャード
BF	ブルギナ・ファソ	GH	ガーナ	MC	モナコ	TG	トーゴー
BG	ブルガリア	GM	ガンビア	MD	モルドヴァ	TJ	タジキスタン
BJ	ベナン	GN	ギニア	MG	マダガスカル	TM	トルクメニスタン
BR	ブラジル	GR	ギリシャ	MK	マケドニア旧ユーゴスラヴィア共和国	TR	トルコ
BY	ベラルーシ	GW	ギニア・ビサオ	ML	マリ	TT	トリニダッド・トバゴ
CA	カナダ	HR	クロアチア	MN	モンゴル	TZ	タンザニア
CF	中央アフリカ	HU	ハンガリー	MR	モーリタニア	UA	ウクライナ
CG	コンゴー	ID	インドネシア	MW	マラウイ	UG	ウガンダ
CH	スイス	IE	アイルランド	MX	メキシコ	US	米国
CI	コートジボアール	IL	イスラエル	MZ	モザンビーク	UZ	ウズベキスタン
CM	カメルーン	IN	インド	NE	ニジェール	VN	ヴェトナム
CN	中国	IS	アイスランド	NL	オランダ	YU	ユーゴースラヴィア
CR	コスタ・リカ	IT	イタリア	NO	ノールウェー	ZA	南アフリカ共和国
CU	キューバ	JP	日本	NZ	ニュー・ジーランド	ZW	ジンバブエ
CY	キプロス	KE	ケニア	PL	ポーランド		
CZ	チェッコ	KG	キルギスタン	PT	ポルトガル		
DE	ドイツ	KP	北朝鮮	RO	ルーマニア		
DK	デンマーク	KR	韓国				

明 細 書

情報処理装置および方法、並びに提供媒体

技術分野

本発明は、情報処理装置および方法、並びに提供媒体に関し、特に、暗号化された情報を利用する情報処理装置および方法、並びに提供媒体に関する。

背景技術

音楽などの情報（コンテンツ）を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザが、その情報処理装置でコンテンツを復号して、利用するシステムがある。

しかしながら、従来のシステムにおいては、ユーザの性別や年齢などの個人情報、コンテンツの利用実績、またはユーザの所有する情報処理装置の種類に応じて、コンテンツの利用を提供するなど、変化に富んだサービスを提供することができない課題があった。

発明の開示

本発明はこのような状況に鑑みてなされたものであり、変化に富んだサービスを提供することができるようにするものである。

かかる課題を解決するため本発明においては、情報処理装置において、暗号化されている第１の情報を保持する保持手段と、第１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報を、第１の情報に対応させて記憶する記憶手段と、保持手段により保持されている暗号化されている第１の情報と、記憶手段により記憶されている第２の情報を所定の機器に送信する送信手段を具備する。

また本発明においては、情報処理方法において、暗号化されている第１の情報

を保持する保持ステップと、第１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報を、第１の情報に対応させて記憶する記憶ステップと、保持ステップで保持された暗号化されている第１の情報と、記憶ステップで記憶された第２の情報を所定の機器に送信する送信ステップを具備する。

さらに本発明においては、提供媒体において、暗号化されている第１の情報を保持する保持ステップと、第１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報を、第１の情報に対応させて記憶する記憶ステップと、保持ステップで保持された暗号化されている第１の情報と、記憶ステップで記憶された第２の情報を所定の機器に送信する送信ステップを具備する処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供する。

さらに本発明においては、情報処理装置、情報処理方法、提供媒体において、暗号化されている第１の情報が保持され、第１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報が、第１の情報に対応されて記憶され、保持された暗号化されている第１の情報と、記憶された第２の情報が所定のプロバイダに送信される。

さらに本発明においては、情報処理装置において、所定のプロバイダから送信されてくる、暗号化されている第１の情報、および第１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報を受信する受信手段と、受信手段により受信された第２の情報に対応して、第１の情報の価格条件と価格条件に対応する価格内容を含む第３の情報を作成する作成手段と、受信手段により受信された暗号化されている第１の情報および第２の情報、並びに作成手段により作成された第３の情報を、所定の機器に送信する送信手段を具備する。

さらに本発明においては、情報処理方法において、所定のプロバイダから送信されてくる、暗号化されている第１の情報、および第１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報を受信する受信ステップと、受信ステップで受信された第２の情報に対応して、第１の情報の価格条件と価格条件に対応する価格内容を含む第３の情報を作成する作成ステップと、受信ステップで受

信された暗号化されている第１の情報および第２の情報、並びに作成ステップで作成された第３の情報を、所定の機器に送信する送信ステップを具備する。

さらに本発明においては、提供媒体において、所定のプロバイダから送信されてくる、暗号化されている第１の情報、および第１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報を受信する受信ステップと、受信ステップで受信された第２の情報に対応して、第１の情報の価格条件と価格条件に対応する価格内容を含む第３の情報を作成する作成ステップと、受信ステップで受信された暗号化されている第１の情報および第２の情報、並びに作成ステップで作成された第３の情報を、所定の機器に送信する送信ステップを具備する処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供する。

さらに本発明においては、情報処理装置、情報処理方法、および提供媒体において、所定のプロバイダから送信されてくる、暗号化されている第１の情報、および第１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報が受信され、受信された第２の情報に対応して、第１の情報の価格条件と価格条件に対応する価格内容を含む第３の情報が作成され、受信された暗号化されている第１の情報および第２の情報、並びに作成された第３の情報が、所定の機器に送信される。

さらに本発明においては、情報処理装置において、所定の基準情報を記憶する記憶手段と、所定のプロバイダから送信されてくる、暗号化されている第１の情報、第１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報、および第１の情報の価格条件と価格条件に対応する価格内容を含む第３の情報を受信する受信手段と、記憶手段に記憶されている基準情報に対応する、受信手段により受信された第２の情報の利用条件を選択する利用条件選択手段と、記憶手段に記憶されている基準情報に対応する、受信手段により受信された第３の情報の価格条件を選択する価格条件選択手段と、利用条件選択手段により選択された利用条件に対応する利用内容に従って、暗号化されている第１の情報を復号して、利用する利用手段と、価格条件選択手段により選択された価格条件に対応する価

格内容に従って、利用手段による利用に対する課金処理を実行する実行手段を具備する。

さらに本発明においては、情報処理方法において、所定の基準情報を記憶する記憶ステップと、所定のプロバイダから送信されてくる、暗号化されている第１の情報、第１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報、および第１の情報の価格条件と価格条件に対応する価格内容を含む第３の情報を受信する受信ステップと、記憶ステップで記憶された基準情報に対応する、受信ステップで受信された第２の情報の利用条件を選択する利用条件選択ステップと、記憶ステップで記憶された基準情報に対応する、受信ステップで受信された第３の情報の価格条件を選択する価格条件選択ステップと、利用条件選択ステップで選択された利用条件に対応する利用内容に従って、暗号化されている第１の情報を復号して、利用する利用ステップと、価格条件選択ステップで選択された価格条件に対応する価格内容に従って、利用ステップでの利用に対する課金処理を実行する実行ステップとを具備する。

さらに本発明においては、提供媒体において、所定の基準情報を記憶する記憶ステップと、所定のプロバイダから送信されてくる、暗号化されている第１の情報、第１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報、および第１の情報の価格条件と価格条件に対応する価格内容を含む第３の情報を受信する受信ステップと、記憶ステップで記憶された基準情報に対応する、受信ステップで受信された第２の情報の利用条件を選択する利用条件選択ステップと、記憶ステップで記憶された基準情報に対応する、受信ステップで受信された第３の情報の価格条件を選択する価格条件選択ステップと、利用条件選択ステップで選択された利用条件に対応する利用内容に従って、暗号化されている第１の情報を復号して、利用する利用ステップと、価格条件選択ステップで選択された価格条件に対応する価格内容に従って、利用ステップでの利用に対する課金処理を実行する実行ステップを具備する処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供する。

さらに本発明においては、情報処理装置、情報処理方法、および提供媒体において、所定の基準情報が記憶され、所定のプロバイダから送信されてくる、暗号化されている第１の情報、第１の情報の利用条件と利用条件に対応する利用内容を含む第２の情報、および第１の情報の価格条件と価格条件に対応する価格内容を含む第３の情報が受信され、記憶されている基準情報に対応する、受信された第２の情報の利用条件が選択され、記憶されている基準情報に対応する、受信された第３の情報の価格条件が選択され、選択された利用条件に対応する利用内容に従って、暗号化されている第１の情報が復号され、利用され、選択された価格条件に対応する価格内容に従って、利用に対する課金処理が実行される。

図面の簡単な説明

図１は、ＥＭＤシステムを説明する系統図である。

図２は、ＥＭＤシステムにおける、主な情報の流れを説明する系統図である。

図３は、ＥＭＤサービスセンタ１の機能的構成を示すブロック図である。

図４は、ＥＭＤサービスセンタ１の配送用鍵Ｋｄの送信を説明する略線図である。

図５は、ＥＭＤサービスセンタ１の配送用鍵Ｋｄの送信を説明する他の略線図である。

図６は、ＥＭＤサービスセンタ１の配送用鍵Ｋｄの送信を説明する他の略線図である。

図７は、ＥＭＤサービスセンタ１の配送用鍵Ｋｄの送信を説明する他の略線図である。

図８は、ＥＭＤサービスセンタ１の配送用鍵Ｋｄの送信を説明する他の図表である。

図９は、システム登録情報を説明する図表である。

図１０は、利用ポイント情報を説明する図表である。

図１１は、コンテンツプロバイダ２の機能的構成例を示すブロック図である。

図１２は、ＵＣＰの例を示す図表である。

図１３は、コンテンツの管理移動を説明する略線図である。

図１４は、第１世代複製を説明する略線図である。

図１５は、サービスコードおよびコンディションコードのコード値の例を示す図表である。

図１６は、ＵＣＰの利用条件として設定されたコード値の例を示す図表である。

図１７は、コンテンツプロバイダセキュアコンテナの例を示す略線図である。

図１８は、コンテンツプロバイダ２の証明書の例を示す略線図である。

図１９は、サービスプロバイダ３の機能的構成を示すブロック図である。

図２０は、ＰＴの例を示す図表である。

図２１は、ＰＴの価格条件として設定されたコード値の例を示す図表である。

図２２は、他のＰＴの例を示す図表である。

図２３は、他のＰＴの価格条件として設定されたコード値の例を示す図表である。

図２４は、サービスプロバイダセキュアコンテナの例を示す略線図である。

図２５は、サービスプロバイダ３の証明書の例を示す略線図である。

図２６は、ユーザホームネットワーク５のレシーバ５１の機能的構成例を示すブロック系統図である。

図２７は、レシーバ５１のＳＡＭ６２の証明書の例を示す略線図である。

図２８は、ＵＣＳの例を示す図表である。

図２９は、レシーバ５１の外部記憶部６３の利用情報記憶部６３Ａの内部を説明する略線図である。

図３０は、課金情報の例を示す図表である。

図３１は、レシーバ５１の記憶モジュール７３に記憶されている情報を示す図表である。

図３２は、基準情報５１を説明する図表である。

図３３は、基準情報５１の利用ポイント情報の例を示す図表である。

図３４は、登録リストの例を示す図表である。

図３５は、ユーザホームネットワーク５のレシーバ２０１の機能的構成例を示すブロック図である。

図３６は、レシーバ２０１の記憶モジュール２２３に記憶されている情報の例を示す図表である。

図３７は、基準情報２０１の例を示す図表である。

図３８は、基準情報５１の利用ポイント情報の例を示す図表である。

図３９は、コンテンツの利用処理を説明するフローチャートである。

図４０は、ＥＭＤサービスセンタ１がコンテンツプロバイダ２へ配送用鍵Ｋｄを送信する処理を説明するフローチャートである。

図４１は、コンテンツプロバイダ２とＥＭＤサービスセンタ１との相互認証の動作を説明するフローチャートである。

図４２は、コンテンツプロバイダ２とＥＭＤサービスセンタ１との相互認証の他の動作を説明するフローチャートである。

図４３は、コンテンツプロバイダ２とＥＭＤサービスセンタ１との相互認証の他の動作を説明するフローチャートである。

図４４は、コンテンツプロバイダ２がサービスプロバイダ３にコンテンツプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

図４５は、サービスプロバイダ３がレシーバ５１にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

図４６は、レシーバ５１がサービスプロバイダセキュアコンテナを受信する処理を説明するフローチャートである。

図４７は、レシーバ５１がコンテンツを再生する処理を説明するフローチャートである。

図４８は、決済処理を説明するフローチャートである。

発明の実施の形態

以下に本発明の実施の形態を説明する。

（１）情報配信システム

図１は、本発明を適用したＥＭＤ（Ｅｌｅｃｔｒｏｎｉｃ　Ｍｕｓｉｃ　Ｄｉｓｔｒｉｂｕｔｉｏｎ：電子音楽配信）システムを説明する図である。ＥＭＤシステムは、各装置を管理するＥＭＤサービスセンタ１、コンテンツを提供するコンテンツプロバイダ２、コンテンツに対応する所定のサービスを提供するサービスプロバイダ３、およびコンテンツが利用される機器（この例の場合、レシーバ５１およびレシーバ２０１）からなるユーザホームネットワーク５から構成されている。

ＥＭＤシステムに登録された機器（例えば、レシーバ５１またはレシーバ２０１）に配信（提供）されるコンテンツ（Ｃｏｎｔｅｎｔ）とは、情報そのものが価値を有するデジタルデータで、この例の場合、１つのコンテンツは、１曲分の音楽データに相当する。ユーザは、コンテンツを購入し（実際は、コンテンツを利用する権利を購入し）、提供されるコンテンツを再生したり、複製して利用する。尚、コンテンツは、音楽データだけでなく、映像データ、ゲームプログラム、コンピュータプログラム、著作権データなどの場合も有りうる。

ＥＭＤサービスセンタ１は、ＥＭＤシステムにおける主な情報の流れを示す図２に示すように、ユーザホームネットワーク５、および複数のコンテンツプロバイダ２（この例の場合、２つのコンテンツプロバイダ２－１，２－２（以下、コンテンツプロバイダ２－１，２－２を個々に区別する必要がない場合、単に、コンテンツプロバイダ２と記述する。他の装置についても同様である））に、コンテンツを利用するために必要な配送用鍵Ｋｄを送信する。ＥＭＤサービスセンタ１はまた、ユーザホームネットワーク５の機器から、課金情報等を受信して、料金を精算したり、コンテンツプロバイダ２からはＵＣＰを、そしてサービスプロバイダ３からＰＴを受信する。

コンテンツプロバイダ２－１，２－２は、提供するコンテンツ（コンテンツ鍵

Ｋｃｏで暗号化されている)、そのコンテンツを復号するために必要なコンテンツ鍵Ｋｃｏ（配送用鍵Ｋｄで暗号化されている)、およびコンテンツの利用内容などを示す取扱方針（以下、ＵＣＰ（Ｕｓａｇｅ　Ｃｏｎｔｒｏｌ　Ｐｏｌｉｃｙ）と記述する）を保持し、それらを、コンテンツプロバイダセキュアコンテナ（後述）と称する形態で、サービスプロバイダ３に供給する。なお、この例の場合、２つのサービスプロバイダ３－１，３－２が存在するものとする。

サービスプロバイダ３－１，３－２は、コンテンツプロバイダ２から供給されるＵＣＰに対応して、１つまたは複数の価格情報（以下、ＰＴ（Ｐｒｉｃｅ　Ｔａｇ）と記述する）を作成し、それを保持する。サービスプロバイダ３は、作成したＰＴを、コンテンツプロバイダ２から供給されたコンテンツ（コンテンツ鍵Ｋｃｏで暗号化されている)、コンテンツ鍵Ｋｃｏ（配送用鍵Ｋｄで暗号化されている)、およびＵＣＰとともに、サービスプロバイダセキュアコンテナと称する形態で、専用のケーブルネットワーク、インターネット、または衛星通信などから構成されるネットワーク４を介して、ユーザホームネットワーク５に送信する。

ユーザホームネットワーク５は、供給されたＵＣＰおよびＰＴに基づいて、使用許諾条件情報（以下、ＵＣＳ（Ｕｓａｇｅ　Ｃｏｎｔｒｏｌ　Ｓｔａｔｕｓ）と称する）を作成し、作成したＵＣＳに基づいてコンテンツを利用する処理を実行する。ユーザホームネットワーク５はまた、ＵＣＳを作成するタイミングで課金情報を作成し、例えば、配送用鍵Ｋｄの供給を受けるタイミングで、対応するＵＣＰおよびＰＴなどとともにＥＭＤサービスセンタ１に送信する。なお、ユーザホームネットワーク５は、ＵＣＰおよびＰＴをＥＭＤサービスセンタ１に送信しないようにすることもできる。

この例の場合、ユーザホームネットワーク５は、図１に示すように、ＨＤＤ５２に接続され、ＳＡＭ（Ｓｅｃｕｒｅ　Ａｐｐｌｉｃａｔｉｏｎ　Ｍｏｄｕｌｅ）６２を有するレシーバ５１、およびＨＤＤ２０２に接続され、ＳＡＭ２１２を有するレシーバ２０１から構成されている。なお、レシーバ５１およびレシーバ

２０１についての詳細は後述する。

（２）ＥＭＤサービスセンタ

図３は、ＥＭＤサービスセンタ１の機能的構成を示すブロック図である。サービスプロバイダ管理部１１は、サービスプロバイダ３に利益分配の情報を供給する。コンテンツプロバイダ管理部１２は、コンテンツプロバイダ２に配送用鍵Ｋｄを送信したり、利益分配の情報を供給する。

著作権管理部１３は、ユーザホームネットワーク５のコンテンツの利用の実績を示す情報を、著作権を管理する団体、例えば、ＪＡＳＲＡＣ（Ｊａｐａｎｅｓｅ Ｓｏｃｉｅｔｙ ｆｏｒ Ｒｉｇｈｔｓ ｏｆ Ａｕｔｈｏｒｓ，Ｃｏｍｐｏｓｅｒｓ ａｎｄ Ｐｕｂｌｉｓｈｅｒｓ：日本音楽著作権協会）に送信する。

鍵サーバ１４は、配送用鍵Ｋｄを記憶しており、それを、コンテンツプロバイダ管理部１２を介してコンテンツプロバイダ２に供給したり、ユーザ管理部１８等を介してユーザホームネットワーク５に供給する。

ユーザホームネットワーク５の、ＥＭＤシステムに正式登録された機器およびコンテンツプロバイダ２に供給される、ＥＭＤサービスセンタ１からの配送用鍵Ｋｄについて、図４乃至図７を参照して説明する。

図４は、コンテンツプロバイダ２がコンテンツの提供を開始し、ユーザホームネットワーク５を構成する、例えば、レシーバ５１がコンテンツの利用を開始する、１９９８年１月における、ＥＭＤサービスセンタ１が有する配送用鍵Ｋｄ、コンテンツプロバイダ２が有する配送用鍵Ｋｄ、およびレシーバ５１が有する配送用鍵Ｋｄを示す図である。

図４の例において、配送用鍵Ｋｄは、暦の月の初日から月の末日まで、使用可能であり、たとえば、所定のビット数の乱数である”ａａａａａａａａ”の値を有するバージョン１である配送用鍵Ｋｄは、１９９８年１月１日から１９９８年１月３１日まで使用可能（すなわち、１９９８年１月１日から１９９８年１月３１日の期間にサービスプロバイダ３を介してユーザホームネットワーク５に配布

されるコンテンツを暗号化するコンテンツ鍵Ｋｃｏは、バージョン１である配送用鍵Ｋｄで暗号化されている）であり、所定のビット数の乱数である”ｂｂｂｂｂｂｂｂ”の値を有するバージョン２である配送用鍵Ｋｄは、１９９８年２月１日から１９９８年２月２８日まで使用可能（すなわち、その期間にサービスプロバイダ３を介してユーザホームネットワーク５に配布されるコンテンツを暗号化するコンテンツ鍵Ｋｃｏは、バージョン２である配送用鍵Ｋｄで暗号化されている）である。同様に、バージョン３である配送用鍵Ｋｄは、１９９８年３月中に使用可能であり、バージョン４である配送用鍵Ｋｄは、１９９８年４月中に使用可能であり、バージョン５である配送用鍵Ｋｄは、１９９８年５月中に使用可能であり、バージョン６である配送用鍵Ｋｄは、１９９８年６月中に使用可能である。

コンテンツプロバイダ２がコンテンツの提供を開始するに先立ち、ＥＭＤサービスセンタ１は、コンテンツプロバイダ２に、１９９８年１月から１９９８年６月まで利用可能な、バージョン１乃至バージョン６の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、記憶する。６ヶ月分の配送用鍵Ｋｄを記憶するのは、コンテンツプロバイダ２が、コンテンツを提供する前のコンテンツおよびコンテンツ鍵の暗号化などの準備に、所定の期間が必要だからである。

また、レシーバ５１がコンテンツの利用を開始するに先立ち、ＥＭＤサービスセンタ１は、レシーバ５１に、１９９８年１月から１９９８年３月まで、利用可能なバージョン１乃至バージョン３である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、記憶する。３ヶ月の配送用鍵Ｋｄを記憶するのは、レシーバ５１が、ＥＭＤサービスセンタ１に接続できないなどのトラブルにより、コンテンツの利用が可能な契約期間にもかかわらずコンテンツが利用できない等の事態を避けるためであり、また、ＥＭＤサービスセンタ１への接続の頻度を低くし、ユーザホームネットワーク５の負荷を低減するためである。

１９９８年１月１日から１９９８年１月３１日の期間には、バージョン１である配送用鍵Ｋｄが、ＥＭＤサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

１９９８年２月１日における、ＥＭＤサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図５で説明する。ＥＭＤサービスセンタ１は、コンテンツプロバイダ２に、１９９８年２月から１９９８年７月まで利用可能な、バージョン２乃至バージョン７の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。ＥＭＤサービスセンタ１は、レシーバ５１に、１９９８年２月から１９９８年４月まで、利用可能なバージョン２乃至バージョン４である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。ＥＭＤサービスセンタ１は、バージョン１である配送用鍵Ｋｄをそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送用鍵Ｋｄを利用できるようにするためである。

１９９８年２月１日から１９９８年２月２８日の期間には、バージョン２である配送用鍵Ｋｄが、ＥＭＤサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

１９９８年３月１日における、ＥＭＤサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図６で説明する。ＥＭＤサービスセンタ１は、コンテンツプロバイダ２に、１９９８年３月から１９９８年８月まで利用可能な、バージョン３乃至バージョン８の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。ＥＭＤサービスセンタ１は、レシーバ５１に、１９９８年３月から１９９８年５月まで、利用可能なバージョン３乃至バージョン５である３つの配送用鍵Ｋｄを送信し、レ

シーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。ＥＭＤサービスセンタ１は、バージョン１である配送用鍵Ｋｄおよびバージョン２である配送用鍵Ｋｄをそのまま記憶する。

１９９８年３月１日から１９９８年３月３１日の期間には、バージョン３である配送用鍵Ｋｄが、ＥＭＤサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

１９９８年４月１日における、ＥＭＤサービスセンタ１の配送用鍵Ｋｄのコンテンツプロバイダ２、およびレシーバ５１への送信を図７で説明する。ＥＭＤサービスセンタ１は、コンテンツプロバイダ２に、１９９８年４月から１９９８年９月まで利用可能な、バージョン４乃至バージョン９の６つの配送用鍵Ｋｄを送信し、コンテンツプロバイダ２は、６つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。ＥＭＤサービスセンタ１は、レシーバ５１に、１９９８年４月から１９９８年６月まで、利用可能なバージョン３乃至バージョン５である３つの配送用鍵Ｋｄを送信し、レシーバ５１は、３つの配送用鍵Ｋｄを受信し、受信前に記憶していた配送用鍵Ｋｄに上書きし、新たな配送用鍵Ｋｄを記憶する。ＥＭＤサービスセンタ１は、バージョン１である配送用鍵Ｋｄ、バージョン２である配送用鍵Ｋｄ、およびバージョン３である配送用鍵Ｋｄをそのまま記憶する。

１９９８年４月１日から１９９８年４月３０日の期間には、バージョン４である配送用鍵Ｋｄが、ＥＭＤサービスセンタ１、コンテンツプロバイダ２、ユーザホームネットワーク５を構成するレシーバ５１で利用される。

このように、あらかじめ先の月の配送用鍵Ｋｄを配布しておくことで、仮にユーザが１，２ヶ月まったくＥＭＤサービスセンタ１にアクセスしなくても、一応、コンテンツの買い取りが行え、時を見計らって、ＥＭＤサービスセンタ１にアクセスして鍵を受信することができる。

また、ユーザホームネットワーク５の、ＥＭＤシステムに正式登録された機器

、およびコンテンツプロバイダ２には、以上のように、３ヶ月分の配送用鍵Ｋｄが配布されるが、ＥＭＤシステムに正式登録されておらず、仮登録（詳細は後述する）されている状態の、ユーザホームネットワーク５の機器には、３ヶ月分の配送用鍵Ｋｄに代わり、図８に示すような、１ヶ月分の配送用鍵Ｋｄが配布される。この例においては、ユーザホームネットワーク５の機器をＥＭＤシステムに正式登録するために、与信処理など、約１ヶ月程度の時間を有する登録手続が必要となる。そこで、登録申請から正式登録されるまでの間（約１ヶ月間）においても、コンテンツの利用が可能となるように、正式登録されていない機器（仮登録されている機器）には、１ヶ月間において利用可能な配送用鍵Ｋｄが配布される。

図３に戻り、経歴データ管理部１５は、ユーザ管理部１８から出力される、課金情報、そのコンテンツに対応するＰＴ、およびそのコンテンツに対応するＵＣＰなどを記憶する。

利益分配部１６は、経歴データ管理部１５から供給された各種情報に基づき、ＥＭＤサービスセンタ１、コンテンツプロバイダ２－１，２－２、およびサービスプロバイダ３－１，３－２の利益をそれぞれ算出し、その結果をサービスプロバイダ管理部１１、コンテンツプロバイダ管理部１２、出納部２０、および著作権管理部１３に出力する。利益配分部１６はまた、算出した利益に応じてコンテンツプロバイダ２－１，２－２およびサービスプロバイダ３－１，３－２のそれぞれに対する利用ポイント（利益が大きければ大きいほど、すなわち、ユーザが利用すればするほど、大きい値となるポイント）を算出し、ユーザ管理部１８に出力する。なお、以下において、コンテンツプロバイダ２における利用ポイントをコンテンツ利用ポイントと称し、サービスプロバイダ３における利用ポイントをサービス利用ポイントと称する。

相互認証部１７は、コンテンツプロバイダ２、サービスプロバイダ３、およびユーザホームネットワーク５の機器と相互認証を実行する。

ユーザ管理部１８は、ＥＭＤシステムに登録可能な、ユーザホームネットワー

ク５の機器に関する情報（以下、システム登録情報と称する）を管理する。システム登録情報には、図９に示すように、「ＳＡＭのＩＤ」、「機器番号」、「決済ＩＤ」、「決済ユーザ情報」、複数の「従属ユーザ情報」、および「利用ポイント情報」の項目に設定される情報が含まれる。

「ＳＡＭのＩＤ」には、製造された、ユーザホームネットワーク５の機器のＳＡＭのＩＤが記憶される。図９のシステム登録情報の「ＳＡＭのＩＤ」には、レシーバ５１のＳＡＭ６２のＩＤおよびレシーバ２０１のＳＡＭ２１２のＩＤが設定されている。

「機器番号」には、ＳＡＭを有するユーザホームネットワーク５の機器に、予め設定された機器番号が設定される。ユーザホームネットワーク５の機器が、ネットワーク４を介してサービスプロバイダ３と、およびＥＭＤサービスセンタ１と直接通信することができる機能を有し（通信部を有し）、かつ、例えば、ＵＣＰやＰＴの内容をユーザに出力（提示）したり、ユーザがＵＣＰの利用内容を選択することができる機能を有している（表示部および操作部を有している）場合、その機器（以下、このような機能を有する機器を主機器と称する）には、１００番以上の機器番号が与えられる。機器が、そのような機能を有しいない場合、その機器（以下、このような機器を従機器と称する）には、９９番以下の機器番号が与えられる。この例の場合、レシーバ５１およびレシーバ２０１の両者は、上述した機能を有しているので、それぞれには、１００番以上の機器番号（１００番）が与えられてる。そこで、図９のシステム登録情報の「機器番号」には、レシーバ５１のＳＡＭ６２のＩＤおよびレシーバ２０１のＳＡＭ２１２のＩＤに対応する「機器番号」のそれぞれには、機器番号１００番が設定されている。

「決済ＩＤ」には、ＥＭＤシステムに正式登録されたとき割り当てられる所定のＩＤが記憶される。この例の場合、レシーバ５１は、ユーザＦが決済ユーザ（後述）として、そしてレシーバ２０１は、ユーザＡを決済ユーザとして、それぞれ正式登録され、決済ＩＤが与えられているので、図９のシステム登録情報の、ＳＡＭ６２のＩＤおよびＳＡＭ２１２のＩＤに対応する「決済ＩＤ」には、与え

られた決済ＩＤが設定されている。

「決済ユーザ情報」には、計上される課金を決済するユーザ（以下、このようなユーザを決済ユーザと称する）の、氏名、住所、電話番号、決済機関情報（例えば、クレジットカード番号等）、生年月日、年齢、性別、ＩＤ、パスワードなどが設定される。

「決済ユーザ情報」に設定される決済ユーザの、氏名、住所、電話番号、決済機関の情報、生年月日、および性別（以下、「決済ユーザ情報」に設定されるこれらの情報を、個々に区別する必要がない場合、まとめて、ユーザ一般情報と称する）は、登録が申請される際にユーザから提供され、設定されるが、この例の場合、そのうちの、氏名、住所、電話番号、および決済機関の情報は、それらに基づいて与信処理が行われるので、正確な情報（例えば、決済機関に登録されている情報）である必要がある。それに対してユーザ一般情報の生年月日、年齢、および性別は、与信処理には用いられないので、この例の場合、それらの情報は、正確である必要はなく、またユーザは、その情報を必ずしも提供する必要がない。「決済ユーザ情報」に記憶される決済ユーザの、ＩＤおよびパスワードは、ＥＭＤシステムに仮登録されるときに割り当てられ、設定される。

この例の場合、レシーバ５１は、ユーザＦが決済ユーザとして登録されているので、図９のシステム登録情報の、ＳＡＭ６２のＩＤに対応する「決済ユーザ情報」には、ユーザＦから提供されたユーザ一般情報、ユーザＦのＩＤ、およびユーザＦのパスワードが設定されている。レシーバ２０１は、ユーザＡが決済ユーザとして登録されているので、ＳＡＭ２１２のＩＤに対応する「決済ユーザ情報」には、ユーザＡから提供されたユーザ一般情報、ユーザＡのＩＤ、およびユーザＡのパスワードが設定されている。なお、この例の場合、ユーザＦは、男性で、ユーザＡは、女性とする。

「従属ユーザ情報」には、課金を決済しないユーザ（以下、このようなユーザを従属ユーザと称する）の、氏名、住所、電話番号、生年月日、年齢、性別、ＩＤ、パスワードなどが設定される。すなわち、「決済ユーザ情報」に設定される情

報のうち、決済機関の情報以外の情報が設定される。従属ユーザに対しては与信処理が行われないので、「従属ユーザ情報」に設定される従属ユーザの、氏名、住所、電話番号、生年月日、年齢、および性別の情報は、正確なものである必要がない。例えば、氏名の場合は、ニックネームのようなものでもよい。また氏名はユーザを特定するために必要とされるが、他の情報は、ユーザは必ずしも提供する必要がない。「従属ユーザ情報」に設定される従属ユーザの、ＩＤおよびパスワードは、仮登録または正式登録されるときに割り当てられ、設定される。

この例の場合、レシーバ５１およびレシーバ２０１の両者には、従属ユーザが登録されていないので、図９のシステム登録情報のＳＡＭ６２のＩＤに対応する「従属ユーザ情報」、およびＳＡＭ２１２のＩＤに対応する「従属ユーザ情報」には、何の情報も設定されていない。

「利用ポイント情報」には、利益分配部１６から出力された利用ポイントが設定される。図１０Ａは、ＳＡＭ６２に対応する「利用ポイント情報」に記憶されているレシーバ５１の利用ポイント情報を示している。これによれば、レシーバ５１のユーザＦ（決済ユーザ）には、コンテンツプロバイダ２－１のコンテンツ利用ポイントが２２２ポイント、コンテンツプロバイダ２－２のコンテンツ利用ポイントが１２３ポイント、サービスプロバイダ３－１のサービス利用ポイントが３４５ポイント、そしてサービスプロバイダ３－２のサービス利用ポイントが０ポイントだけ与えられている。

図１０Ｂは、ＳＡＭ２１２に対応する「利用ポイント情報」に記憶されているレシーバ２０１の利用ポイント情報を示している。これによれば、レシーバ２０１のユーザＡ（決済ユーザ）には、コンテンツプロバイダ２－１のコンテンツ利用ポイントが２３ポイント、コンテンツプロバイダ２－２のコンテンツ利用ポイントが２２ポイント、サービスプロバイダ３－１のサービス利用ポイントが４０ポイント、そしてサービスプロバイダ３－２のサービス利用ポイントが５ポイントだけ与えられている。

なお、この例において、コンテンツプロバイダ２－１およびコンテンツプロバ

イダ２－２のそれぞれのコンテンツ利用ポイントの合計ポイント（ユーザＦの場合は３４５（＝１２３＋２２２）、ユーザＡの場合は４５ポイント（＝２３＋２２））と、サービスプロバイダ３－１およびサービスプロバイダ３－２のそれぞれのサービス利用ポイントの合計ポイント（ユーザＦの場合は３４５（＝３４５＋０、ユーザＡの場合は４５ポイント（＝５＋４０））が等しくなるようになされている。

ユーザ管理部１８は、このようなシステム登録情報を管理する他、所定の処理に対応して登録リスト（後述）を作成し、配送用鍵Ｋｄとともにユーザホームネットワーク５に送信する。

図３に、再度戻り、課金請求部１９は、経歴データ管理部１５から供給された、課金情報、ＵＣＰ、およびＰＴに基づき、ユーザへの課金を算出し、その結果を、出納部２０に供給する。出納部２０は、ユーザ、コンテンツプロバイダ２、およびサービスプロバイダ３への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決算処理を実行する。出納部２０はまた、決算処理の結果をユーザ管理部１８に通知する。

監査部２１は、ユーザホームネットワーク５の機器から供給された課金情報、ＰＴ、およびＵＣＰの正当性（すなわち、不正をしていないか）を監査する。なお、この場合、ＥＭＤサービスセンタ１は、コンテンツプロバイダ２からのＵＣＰを、サービスプロバイダ３からのＰＴを、そしてユーザホームネットワーク５からのＵＣＰとＰＴを、それぞれ受け取る。

（３）コンテンツプロバイダ

図１１は、コンテンツプロバイダ２－１の機能的構成を示すブロック図である。コンテンツサーバ３１は、ユーザに供給するコンテンツを記憶し、ウォータマーク付加部３２に供給する。ウォータマーク付加部３２は、コンテンツサーバ３１から供給されたコンテンツにウォータマーク（電子透かし）を付加し、圧縮部３３に供給する。

圧縮部３３は、ウォータマーク付加部３２から供給されたコンテンツを、ＡＴ

ＲＡＣ２（Ａｄａｐｔｉｖｅ Ｔｒａｎｓｆｏｒｍ Ａｃｏｕｓｔｉｃ Ｃｏｄｉｎｇ ２）（商標）等の方式で圧縮し、暗号化部３４に供給する。暗号化部３４は、圧縮部３３で圧縮されたコンテンツを、乱数発生部３５から供給された乱数を鍵（以下、この乱数をコンテンツ鍵Ｋｃｏと称する）として、ＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部３８に出力する。

乱数発生部３５は、コンテンツ鍵Ｋｃｏとなる所定のビット数の乱数を暗号化部３４および暗号化部３６に供給する。暗号化部３６は、コンテンツ鍵ＫｃｏをＥＭＤサービスセンタ１から供給された配送用鍵Ｋｄを使用して、ＤＥＳなどの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部３８に出力する。

ＤＥＳは、５６ビットの共通鍵を用い、平文の６４ビットを１ブロックとして処理する暗号方式である。ＤＥＳの処理は、平文を攪拌し、暗号文に変換する部分（データ攪拌部）と、データ攪拌部で使用する鍵（拡大鍵）を共通鍵から生成する部分（鍵処理部）からなる。ＤＥＳのすべてのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

まず、平文の６４ビットは、上位３２ビットのH_0、および下位３２ビットのL_0に分割される。鍵処理部から供給された４８ビットの拡大鍵K_1、および下位３２ビットのL_0を入力とし、下位３２ビットのL_0を攪拌したＦ関数の出力が算出される。Ｆ関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の２種類の基本変換から構成されている。次に、上位３２ビットのH_0と、Ｆ関数の出力が排他的論理和され、その結果はL_1とされる。L_0は、H_1とされる。

上位３２ビットのH_0および下位３２ビットのL_0を基に、以上の処理を１６回繰り返し、得られた上位３２ビットのH_{16}および下位３２ビットのL_{16}が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

ポリシー記憶部３７は、コンテンツに対応して設定されるＵＣＰを記憶し、セキュアコンテナ作成部３８に出力する。図１２は、コンテンツサーバ３１に保持されているコンテンツＡに対応して設定され、ポリシー記憶部３７に記憶されているＵＣＰＡ、Ｂを表している。ＵＣＰには、「コンテンツのＩＤ」、「コンテンツプロバイダのＩＤ」、「ＵＣＰのＩＤ」、「ＵＣＰの有効期限」、「利用条件」、「利用内容」の各項目に設定される情報が含まれる。「コンテンツのＩＤ」には、ＵＣＰが対応するコンテンツのＩＤが設定される。ＵＣＰＡ（図１２Ａ）およびＵＣＰＢ（図１２Ｂ）のそれぞれの「コンテンツのＩＤ」には、コンテンツＡのＩＤが設定されている。

「コンテンツプロバイダのＩＤ」には、コンテンツの提供元のコンテンツプロバイダのＩＤが設定される。ＵＣＰＡおよびＵＣＰＢのそれぞれの「コンテンツプロバイダのＩＤ」には、コンテンツプロバイダ２－１のＩＤが設定されている。「ＵＣＰのＩＤ」には、各ＵＣＰに割り当てられた所定のＩＤが設定され、ＵＣＰＡの「ＵＣＰのＩＤ」には、ＵＣＰＡのＩＤが、ＵＣＰＢの「ＵＣＰのＩＤ」には、ＵＣＰＢのＩＤが、それぞれ設定されている。「ＵＣＰの有効期限」には、ＵＣＰの有効期限を示す情報が設定され、ＵＣＰＡの「ＵＣＰの有効期限」には、ＵＣＰＡの有効期限が、ＵＣＰＢの「ＵＣＰの有効期限」には、ＵＣＰＢの有効期限が、それぞれ設定されている。

「利用条件」は、「ユーザ条件」および「機器条件」の項目からなり、「ユーザ条件」には、このＵＣＰを選択することができるユーザの条件が設定され、「機器条件」には、このＵＣＰを選択することができる機器の条件が設定される。

ＵＣＰＡの場合、「利用条件１０」が設定され、「利用条件１０」の「ユーザ条件１０」には、利用ポイントが２００ポイント以上であることが条件であることを示す情報（”２００ポイント以上”）が設定されている。また「利用条件１０」の「機器条件１０」には、条件がないことを示す情報（”条件なし”）が設定されている。すなわち、ＵＣＰＡは、２００ポイント以上のコンテンツプロバイダ２－１のコンテンツ利用ポイントを有するユーザのみが選択可能となる。

ＵＣＰＢの場合、「利用条件２０」が設定され、「利用条件２０」の「ユーザ条件２０」には、利用ポイントが２００ポイントより少ないことが条件であることをを示す情報（”２００ポイントより少ない”）が設定されている。また「利用条件２０」の「機器条件２０」には、”条件なし”が設定されている。すなわち、ＵＣＰＢは、２００ポイントより少ないコンテンツプロバイダ２－１のコンテンツ利用ポイントを有するユーザのみが選択可能となる。

「利用内容」は、「ＩＤ」、「形式」、「パラメータ」、および「管理移動許可情報」などの項目からなり、その「ＩＤ」には、「利用内容」に設定される情報に割り当てられた所定のＩＤが設定される。「形式」には、再生や複製など、コンテンツの利用形式を示す情報が設定される。「パラメータ」には、「形式」に設定された利用形式に対応する所定の情報が設定される。

「管理移動許可情報」には、コンテンツの管理移動が可能か否か（許可されているか否か）を示す情報（”可”または”不可”）が設定されている。コンテンツの管理移動が行われると、図１３Ａに示すように、管理移動元の機器にコンテンツが保持されつつ、管理移動先の機器にそのコンテンツが移動される。すなわち、管理移動元の機器と管理移動先の機器の両方において、コンテンツが利用される。この点で、図１３Ｂに示すように、移動元の機器にコンテンツが保持されず、移動先の機器のみにコンテンツが保持され、移動先の機器においてのみコンテンツが利用される、通常の移動とは異なる。

また、コンテンツの管理移動が行われている間、管理移動元の機器は、図１３Ａに示すように、他の機器にコンテンツを管理移動することができない（許可されていない）。すなわち、管理移動元の機器と管理移動先の機器の２機においてのみコンテンツが保持される。この点で、図１４Ａに示すように、オリジナルのコンテンツから、複数の複製（第１世代）を作成することができる、第１世代の複製とも異なる。また、管理移動元の機器からコンテンツを戻すことより、他の機器にコンテンツを管理移動することができるので、この点で、図１４Ｂに示すように、１回だけの複製とも異なる。

図１２Ａに戻り、ＵＣＰＡには、４つの「利用内容１１」乃至「利用内容１４」が設けられており、「利用内容１１」において、その「ＩＤ１１」には、「利用内容１１」に割り当てられた所定のＩＤが設定されている。「形式１１」には、コンテンツを買い取って再生する利用形式を示す情報（”買い取り再生”）が設定され、「パラメータ１１」には、”買い取り再生”に対応する所定の情報が設定されている。「管理移動許可情報１１」には、コンテンツの管理移動が許可されていることを示す情報（”可”）が設定されている。

「利用内容１２」において、その「ＩＤ１２」には、「利用内容１２」に割り当てられた所定のＩＤが設定されている。「形式１２」には、第１世代の複製を行う利用形式を示す情報（”第１世代複製”）が設定されている。第１世代複製は、図１４Ａに示したように、オリジナルのコンテンツから、複数の第１世代の複製を作成することができる。ただし、第１世代の複製から第２世代の複製を作成することはできない（許可されていない）。「パラメータ１２」には、”第１世代複製”に対応する所定の情報が設定されている。「管理移動許可情報１２」には、コンテンツの管理移動が許可されていないことを示す”不可”が設定されている。

「利用内容１３」において、その「ＩＤ１３」には、「利用内容１３」に割り当てられた所定のＩＤが設定されている。「形式１３」には、所定の期間（時間）に限って再生する利用形式を示す情報（”期間制限再生”）が設定され、「パラメータ１３」には、”期間制限再生”に対応して、その期間の開始時期（時刻）と終了時期（時刻）が設定されている。「管理移動許可情報１３」には、”不可”が設定されている。

「利用内容１４」において、その「ＩＤ１４」には、「利用内容１４」に割り当てられた所定のＩＤが設定されている。「形式１４」には、５回の複製を行う利用形式（いわゆる、５回複製することができる回数券）を示す情報（”Ｐａｙ Ｐｅｒ Ｃｏｐｙ５”）が設定されている。なお、この場合も、図１４のＢに示すように、複製からの複製を作成することはできない（許可されていない）。「パラメータ１４」には、”Ｐａｙ Ｐｅｒ Ｃｏｐｙ５”に対応して、複製が５回可能

であることを示す情報”複製５回”が設定されている。「管理移動許可情報１４」には、”不可”が設定されている。

図１２ＢのＵＣＰＢには、２つの「利用内容２１」および「利用内容２２」が設けられている。「利用内容２１」において、その「ＩＤ２１」には、「利用内容２１」に割り当てられた所定のＩＤが設定されている。「形式２１」には、４回の再生を行う利用形式を示す情報（”Ｐａｙ　Ｐｅｒ　Ｐｌａｙ４”）が設定され、「パラメータ２１」には、再生が４回可能であることを示す情報（”再生４回”）が設定されている。「管理移動許可情報２１」には、”不可”が設定されている。

「利用内容２２」において、その「ＩＤ２２」には、「利用内容２２」に割り当てられた所定のＩＤが設定されている。「形式２２」には、”Ｐａｙ　Ｐｅｒ　Ｃｏｐｙ２”が設定され、「パラメータ２２」には、”複製２回”が設定されている。「管理移動許可情報２２」には、”不可”が設定されている。

ここで、ＵＣＰＡおよびＵＣＰＢの内容を比較すると、２００ポイント以上の利用ポイントを有するユーザは、４通りの利用内容１１乃至利用内容１４から利用内容を選択することができるのに対して、２００ポイントより少ない利用ポイントを有するユーザは、２通りの利用内容２１，２２からしか利用内容を選択することができないものとされている。

ところで、図１２は、ＵＣＰＡおよびＵＣＰＢを模擬的に表しているが、例えば、ＵＣＰＡの「利用条件１０」およびＵＣＰＢの「利用条件２０」は、図１５Ａに示すサービスコード、および図１５Ｂに示すコンディションコードの他、サービスコードに対応して数値や所定の種類を示すバリューコードにより、実際は構成されている。

図１６Ａは、ＵＣＰＡ（図１２Ａ）の「利用条件１０」の「ユーザ条件１０」および「機器条件１０」として設定されている各コードのコード値を表している。ＵＣＰＡの「利用条件１０」の「ユーザ条件１０」は、”２００ポイント以上”とされているので、”利用ポイントに関し条件有り”を意味する８０ｘｘｈのサー

ビスコード（図１５Ａ）が、このとき数値２００を示す００００Ｃ８ｈのバリューコードが、そして”＞＝（以上)”を意味する０６ｈのコンディションコード（図１５Ｂ）が、ユーザ条件として設定されている。

ＵＣＰＡの「機器条件１０」は、”条件なし”とされているので、”条件なし”を意味する００００ｈのサービスコードが、このとき何ら意味を持たないＦＦＦＦＦＦｈのバリューコードが（図１５Ａ)、そして”無条件”を意味する００ｈのコンディションコード（図１５Ｂ）が、機器条件として設定されている。

図１６Ｂは、ＵＣＰＢの「利用条件２０」の「ユーザ条件２０」および「機器条件２０」として設定されている各コードのコード値を表している。「ユーザ条件２０」は、”２００ポイントより少ない”とされているので、”利用ポイントに関し条件有り”を意味する８０ｘｘｈのサービスコードが、数値２００を示す００００Ｃ８ｈのバリューコード（図１５Ａ）が、そして”＜（より小さい)”を意味する０３ｈのコンディションコード（図１５Ｂ）が、ユーザ条件として設定されている。

ＵＣＰＢの「機器条件２０」は、ＵＣＰＡの「機器条件１０」と同様に、”条件なし”とされ、同一のコード値が設定されているので、その説明は省略する。

図１１に戻り、セキュアコンテナ作成部３８は、例えば、図１７に示すような、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている)、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている)、ＵＣＰＡ，Ｂ、および署名からなるコンテンツプロバイダセキュアコンテナを作成する。なお、署名は、送信したいデータ（この場合、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている)、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている)、およびＵＣＰＡ，Ｂの全体）にハッシュ関数を適用して得られたハッシュ値が、コンテンツプロバイダの公開鍵暗号の秘密鍵（この場合、コンテンツプロバイダ２－１の秘密鍵Ｋｓｃｐ）で暗号化されたものである。

セキュアコンテナ作成部３８はまた、コンテンツプロバイダセキュアコンテナに、図１８に示すコンテンツプロバイダ２－１の証明書を付してサービスプロバ

イダ３に送信する。この証明書は、証明書のバージョン番号、認証局がコンテンツプロバイダ２－１に対し割り付けた証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、およびコンテンツプロバイダ２－１の名前、コンテンツプロバイダ２－１の公開鍵Ｋｐｃｐ、並びにその署名（認証局の秘密鍵Ｋｓｃａで暗号化されている）から構成されている。

署名は、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵で暗号化して作成される。

ハッシュ関数および署名の照合について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの１ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。

署名とデータを受信した受信者は、署名を公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）を得る。さらに受信されたデータのハッシュ値が計算され、計算されたハッシュ値と、署名を復号して得られたハッシュ値とが、等しいか否かが判定される。送信されたデータのハッシュ値と復号したハッシュ値が等しいと判定された場合、受信したデータは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されたデータであることがわかる。署名のハッシュ関数としては、ＭＤ（Ｍｅｓｓａｇｅ　Ｄｉｇｅｓｔ）４，ＭＤ５，ＳＨＡ（Ｓｅｃｕｒｅ　Ｈａｓｈ　Ａｌｇｏｒｉｔｈｍ）－１などが用いられる。

次に公開鍵暗号について説明する。暗号化および復号で同一の鍵（共通鍵）を使用する共通鍵暗号方式に対し、公開鍵暗号方式は、暗号化に使用する鍵と復号するときの鍵が異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開しても良い鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

公開鍵暗号の中で代表的なＲＳＡ（Ｒｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｌｅｍａｎ）暗号を、簡単に説明する。まず、２つの十分に大きな素数であるｐおよびｑを求め、さらにｐとｑの積であるｎを求める。（ｐ－１）と（ｑ－１）の最小公倍数Ｌを算出し、更に、３以上Ｌ未満で、かつ、Ｌと互いに素な数ｅを求める（すなわち、ｅとＬを共通に割り切れる数は、１のみである)。

次に、Ｌを法とする乗算に関するｅの乗法逆元ｄを求める。すなわち、ｄ，ｅ、およびＬの間には、$ed = 1 \mod L$が成立し、ｄはユークリッドの互除法で算出できる。このとき、ｎとｅが公開鍵とされ、ｐ，ｑ，およびｄが、秘密鍵とされる。

暗号文Ｃは、平文Ｍから、式（１）の処理で算出される。

$$C = M^e \mod n \qquad (1)$$

暗号文Ｃは、式（２）の処理で平文Ｍに、復号される。

$$M = C^d \mod n \qquad (2)$$

証明は省略するが、ＲＳＡ暗号で平文を暗号文に変換して、それが復号できるのは、フェルマーの小定理に根拠をおいており、式（３）が成立するからである。

$$M = C^d = (M^e)^d = M^{ed} = M \mod n \qquad (3)$$

秘密鍵ｐとｑを知っているならば、公開鍵ｅから秘密鍵ｄは算出できるが、公開鍵ｎの素因数分解が計算量的に困難な程度に公開鍵ｎの桁数を大きくすれば、公開鍵ｎを知るだけでは、公開鍵ｅから秘密鍵ｄは計算できず、復号できない。以上のように、ＲＳＡ暗号では、暗号化に使用する鍵と復号するときの鍵を、異

なる鍵とすることができる。

また、公開鍵暗号の他の例である楕円曲線暗号（Ｅｌｌｉｐｔｉｃ Ｃｕｒｖｅ Ｃｒｙｐｔｏｇｒａｐｈｙ）についても、簡単に説明する。楕円曲線$y^2=x^3+ax+b$上の、ある点をＢとする。楕円曲線上の点の加算を定義し、ｎＢは、Ｂをｎ回加算した結果を表す。同様に、減算も定義する。ＢとｎＢからｎを算出することは、困難であることが証明されている。ＢとｎＢを公開鍵とし、ｎを秘密鍵とする。乱数ｒを用いて、暗号文Ｃ１およびＣ２は、平文Ｍから、公開鍵で式（４）および式（５）の処理で算出される。

$$C1=M+rnB \qquad (4)$$

$$C2=rB \qquad (5)$$

暗号文Ｃ１およびＣ２は、式（６）の処理で平文Ｍに、復号される。

$$M=C1-nC2 \qquad (6)$$

復号できるのは、秘密鍵ｎを有するものだけである。以上のように、ＲＳＡ暗号と同様に、楕円曲線暗号でも、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

図１１に、再び戻り、コンテンツプロバイダ２－１の相互認証部３９は、ＥＭＤサービスセンタ１から配送用鍵Ｋｄの供給を受けるのに先立ち、ＥＭＤサービスセンタ１と相互認証し、また、相互認証部３９は、サービスプロバイダ３へのコンテンツセキュアコンテナの送信に先立ち、サービスプロバイダ３と相互認証することも可能であるが、この例の場合、コンテンツプロバイダセキュアコンテナには、秘密にしなければならない情報が含まれていないので、この相互認証は、必ずしも必要とされない。

コンテンツプロバイダ２－２は、コンテンツプロバイダ２－１と基本的の同様の構成を有しているので、その図示および説明は省略する。

（４）サービスプロバイダ

次に、図１９のブロック図を参照して、サービスプロバイダ３－１の機能的構成を説明する。コンテンツサーバ４１は、コンテンツプロバイダ２から供給されたコンテンツプロバイダセキュアコンテナに含まれる、コンテンツ（コンテンツ鍵Ｋｃｏで暗号化されている）、コンテンツ鍵Ｋｃｏ（配送用鍵Ｋｄで暗号化されている）、ＵＣＰ、およびコンテンツプロバイダ２の署名を記憶し、セキュアコンテナ作成部４４に供給する。

値付け部４２は、コンテンツプロバイダ２から供給されたコンテンツプロバイダセキュアコンテナに含まれる署名に基づいて、コンテンツプロバイダセキュアコンテナの正当性を検証するが、この場合、コンテンツプロバイダ２の証明書が検証され、正当であるとき、コンテンツプロバイダ２の公開鍵が取得される。そしてこの取得された公開鍵に基づいて、コンテンツプロバイダセキュアコンテナの正当性が検証される。

コンテンツプロバイダセキュアコンテナの正当性を確認すると、値付け部４２は、コンテンツプロバイダセキュアコンテナに含まれるＵＣＰに対応する、ＰＴを作成し、セキュアコンテナ作成部４４に供給する。図２０は、図１２ＡのＵＣＰＡに対応して作成された、２つのＰＴＡ－１（図２０Ａ）およびＰＴＡ－２（図２０Ｂ）を表している。ＰＴには、「コンテンツのＩＤ」、「コンテンツプロバイダのＩＤ」、「ＵＣＰのＩＤ」、「サービスプロバイダのＩＤ」、「ＰＴのＩＤ」、「ＰＴの有効期限」、「価格条件」、および「価格内容」の各項目に設定される情報が含まれる。

ＰＴの、「コンテンツのＩＤ」、「コンテンツプロバイダのＩＤ」、および「ＵＣＰのＩＤ」には、ＵＣＰに対応する各項目の情報が、それぞれ設定される。すなわち、ＰＴＡ－１およびＰＴＡ－２のそれぞれの「コンテンツのＩＤ」には、コンテンツＡのＩＤが、それぞれの「コンテンツプロバイダのＩＤ」には、コンテ

ンツプロバイダ２－１のＩＤが、そしてそれぞれの「ＵＣＰのＩＤ」には、ＵＣＰＡのＩＤが設定されている。

「サービスプロバイダのＩＤ」には、ＰＴの提供元のサービスプロバイダ３のＩＤが設定される。ＰＴＡ－１およびＰＴＡ－２の「サービスプロバイダのＩＤ」には、サービスプロバイダ３－１のＩＤが設定されている。「ＰＴのＩＤ」には、各ＰＴに割り当てられた所定のＩＤが設定される。ＰＴＡ－１の「ＰＴのＩＤ」には、ＰＴＡ－１のＩＤが、ＰＴＡ－２の「ＰＴのＩＤ」には、ＰＴＡ－２のＩＤがそれぞれ設定されている。「ＰＴの有効期限」には、ＰＴの有効期限を示す情報が設定される。ＰＴＡ－１の「ＰＴの有効期限」には、ＰＴＡ－１の有効期限が、ＰＴＡ－２の「ＰＴの有効期限」には、ＰＴＡ－２の有効期限が設定されている。

「価格条件」は、ＵＣＰの「利用条件」と同様に、「ユーザ条件」および「機器条件」の項目からなり、その「ユーザ条件」には、このＰＴを選択することができるユーザの条件が設定され、その「機器条件」には、このＰＴを選択することができる機器の条件が設定される。

ＰＴＡ－１の場合、「価格条件１０」が設定され、「価格条件１０」の「ユーザ条件１０」には、ユーザが男性であるを示す情報（”男性”）が設定され、その「機器条件１０」には、”条件なし”が設定されている。すなわち、ＰＴＡ－１は、男性のユーザのみが選択可能となる。

ＰＴＡ－１の「価格条件１０」の「ユーザ条件１０」および「機器条件１０」も、実際は、図２１Ａに示すように、各種コードのコード値が設定されている。「価格条件１０」の「ユーザ条件１０」には、”性別条件有り”を意味する０１ｘｘｈのサービスコード（図１５Ａ）が、このとき男性を意味する０００００ｈのバリューコードが、そして”＝”を意味する０１ｈのコンディションコード（図１５Ｂ）が設定されている。「機器条件１０」には、”条件なし”を意味する０００００ｈのサービスコードが、この場合何ら意味を持たないＦＦＦＦＦＦｈのバリューコードが、そして”無条件”を意味する００ｈのコンディションコード

が設定されている。

ＰＴＡ－２の場合、「価格条件２０」が設定され、「価格条件２０」の「ユーザ条件２０」には、ユーザが女性であることを示す情報（”女性”）が設定され、その「機器条件２０」には、”条件なし”が設定されている。すなわち、ＰＴＡ－２は、女性のユーザのみが選択可能となる。

ＰＴＡ－２の「価格条件２０」の「ユーザ条件２０」および「機器条件２０」も、実際は、図２１Ｂに示すように、各コードのコード値が設定されている。「価格条件２０」の「ユーザ条件２０」には、”性別条件有り”を意味する０１ｘｘｈのサービスコード（図１５Ａ）が、この場合女性を示す０００００１ｈのバリューコードが、そして”＝”を意味する０１ｈのコンディションコード（図１５Ｂ）が設定されている。その「機器条件２０」には、”条件なし”を意味する００００ｈのサービスコードが、この場合何ら意味を持たないＦＦＦＦＦＦｈのバリューコードが、そして”無条件”を意味する００ｈのコンディションコードが設定されている。

図２０に戻り、ＰＴの「価格内容」には、コンテンツが、対応するＵＣＰの「利用内容」の「形式」に設定された利用形式で利用される場合の利用料金が示されている。すなわち、ＰＴＡ－１の「価格内容１１」に設定された”２０００円”およびＰＴＡ－２の「価格内容２１」に設定された”１０００円”は、ＵＣＰＡ（図１２Ａ）の「利用内容１１」の「形式１１」が”買い取り再生”とされているので、コンテンツＡの買い取り価格（料金）を示している。

ＰＴＡ－１の「価格内容１２」の”６００円”およびＰＴＡ－２の「価格内容２２」の”３００円”は、ＵＣＰＡの「利用内容１２」の「形式１２」より、第１世代複製の利用形式でコンテンツＡを利用する場合の料金を示している。ＰＴＡ－１の「価格内容１３」の”１００円”およびＰＴＡ－２の「価格内容２３」の”５０円”は、ＵＣＰＡの「利用内容１３」の「形式１３」より、期間制限再生の利用形式でコンテンツＡを利用する場合の料金を示している。ＰＴＡ－１の「価格内容１４」の”３００円”およびＰＴＡ－２の「価格内容２４」の”１５

０円”は、ＵＣＰＡの「利用内容１４」の「形式１４」より、５回の複製を行う利用形式でコンテンツＡを利用する場合の料金を示している。

なお、この例の場合、ＰＴＡ－１（男性ユーザに適用される）の価格内容と、ＰＴＡ－２（女性ユーザに適用される）の価格内容を比較すると、ＰＴＡ－１の価格内容に示される価格が、ＰＴＡ－２の価格内容に示される価格の２倍に設定されている。例えば、ＵＣＰＡの「利用内容１１」に対応するＰＴＡ－１の「価格内容１１」が”２０００円”とされているのに対し、同様にＵＣＰＡの「利用内容１１」に対応するＰＴＡ－２の「価格内容２１」は”１０００円”とされている。同様、ＰＴＡ－１の「価格内容１２」乃至「価格内容１４」に設定されている価格は、ＰＴＡ－２の「価格内容２２」乃至「価格内容２４」に設定されている価格のそれぞれの２倍とされている。すなわち、女性ユーザは、男性ユーザに比べ、コンテンツＡを、半額の料金で利用することができる。

図２２は、図１２ＢのＵＣＰＢに対応して作成された、２つのＰＴＢ－１およびＰＴＢ－２を表している。図２２ＡのＰＴＢ－１には、コンテンツＡのＩＤ、コンテンツプロバイダ２－１のＩＤ、ＵＣＰＢのＩＤ、ＵＣＰＢの有効期限、サービスプロバイダ３－１のＩＤ、ＰＴＢ－１のＩＤ、ＰＴＢ－１の有効期限、価格条件３０、２通りの価格内容３１，３２などが含まれている。

ＰＴＢ－１の「価格条件３０」の「ユーザ条件３０」には”条件なし”が設定され、「機器条件３０」には、機器が従機器であることを示す情報（”従機器”）が設定されている。すなわち、ＰＴＢ－１は、コンテンツＡが従機器において利用される場合にのみ選択可能となる。

ＰＴＢ－１の「価格条件３０」の「ユーザ条件３０」および「機器条件３０」にも、実際は、図２３Ａに示すように、各コードのコード値が設定されている。「ユーザ条件３０」には、”条件なし”を意味する０００００ｈのサービスコード（図１５Ａ）が、この場合何ら意味を持たないＦＦＦＦＦＦｈのバリューコードが、そして”無条件”を意味する００ｈのコンディションコード（図１５Ｂ）が設定されている。「機器条件３０」は、”従機器”とされているので、”機器に関

し条件有り”を意味する００ｘｘｈのサービスコードが、このとき”数値１００”を示す０００００６４ｈのバリューコードが、そして”＜（小さい）”を意味する０３ｈのコンディションコードが設定されている。この例の場合、従機器には、１００番より小さい機器番号が設定されているので、このようなコード値が設定される。

ＰＴＢ－１の「価格内容３１」の”１００円”は、ＵＣＰＢ（図１２Ｂ）の「利用内容２１」の「形式２１」が”Ｐａｙ　Ｐｅｒ　Ｐｌａｙ４”とされているので、４回の再生を行う場合の料金を示し、「価格内容３２」の”３００円”は、ＵＣＰＢの「利用内容２２」の「形式２２」が”Ｐａｙ　Ｐｅｒ　Ｃｏｐｙ２”とされているので、２回の複製を行う場合の料金を示している。

ＵＣＰＢに対応して作成された、もう一方の図２２ＢのＰＴＢ－２には、コンテンツＡのＩＤ、コンテンツプロバイダ２－１のＩＤ、ＵＣＰＢのＩＤ、サービスプロバイダ３－１のＩＤ、ＰＴＢ－２のＩＤ、ＰＴＢ－２の有効期限、価格条件４０、および２通りの価格内容４１，４２などが含まれている。

ＰＴＢ－２の「価格条件４０」の「ユーザ条件４０」には”条件なし”が設定され、その「機器条件４０」には、機器が主機器であることを条件とする情報（”主機器”）が設定されている。すなわち、ＰＴＢ－２は、主機器においてコンテンツＡが利用される場合にのみ選択可能となる。

ＰＴＢ－２の「価格条件４０」の「ユーザ条件４０」および「機器条件４０」にも、実際は、図２３Ｂに示すように、各コードのコード値が設定されている。「価格条件４０」の「ユーザ条件４０」には、”条件なし”を意味する０００００ｈのサービスコード（図１５Ａ）が、この場合何ら意味を持たないＦＦＦＦＦＦｈのバリューコードが、そして”無条件”を意味する００ｈのコンディションコード（１５Ｂ）が設定されている。「機器条件４０」には、”機器に関し条件有り”を意味する００ｘｘｈのサービスコードが、このとき”数値１００”を示す０００００６４ｈのバリューコードが、そして”＝＞（以上）”を意味する０６ｈのコンディションコードが設定されている。

ＰＴＢ－２の「価格内容４１」および「価格内容４２」のそれぞれに示される価格は、ＵＣＰＢの「利用内容２１」の「形式２１」および「利用内容２２」の「形式２２」のそれぞれに示される利用形式でコンテンツＡを利用する場合の料金を示している。

ここで、ＰＴＢ－１（従機器に適用される）の価格内容とＰＴＢ－２（主機器に適用される）の価格内容を比較すると、ＰＴＢ－１の価格内容は、ＰＴＢ－２の価格内容の２倍に設定されている。例えば、ＰＴＢ－１の「価格内容３１」が”１００円”とされているのに対し、ＰＴＢ－２の「価格内容４１」は５０円とされており、「価格内容３２」が”３００円”とされているのに対して、「価格内容４２」は”１５０円”とされている。

図１９に戻り、ポリシー記憶部４３は、コンテンツプロバイダ２から供給された、コンテンツのＵＣＰを記憶し、セキュアコンテナ作成部４４に供給する。

セキュアコンテナ作成部４４は、例えば、図２４に示すような、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、ＵＣＰＡ，Ｂ、コンテンツプロバイダ２の署名、ＰＴＡ－１，Ａ－２，Ｂ－１，Ｂ－２、およびサービスプロバイダ３の署名からなるサービスプロバイダセキュアコンテナを作成する。

セキュアコンテナ作成部４４はまた、作成したサービスプロバイダセキュアコンテナを、図２５に示すような、証明書のバージョン番号、認証局がサービスプロバイダ３－１に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ３－１の名前、サービスプロバイダ３－１の公開鍵Ｋｐｓｐ、並びに認証局の署名より構成されるサービスプロバイダの証明書を付して、ユーザホームネットワーク５に供給する。

図１９に、再び戻り、相互認証部４５は、コンテンツプロバイダ２からコンテンツプロバイダセキュアコンテナの供給を受け取るのに先立ち、コンテンツプロバイダ２と相互認証する。相互認証部４５また、ユーザホームネットワーク５へ

のサービスプロバイダセキュアコンテナの送信に先立ち、ユーザホームネットワーク５と相互認証するが、このサービスプロバイダ３とユーザホームネットワーク５との相互認証は、例えば、ネットワーク４が衛星通信である場合、実行されない。なお、この例の場合、コンテンツプロバイダセキュアコンテナおよびサービスプロバイダセキュアコンテナには、特に、秘密情報が含まれていないので、サービスプロバイダ３は、コンテンツプロバイダ２およびユーザホームネットワーク５と相互認証を行わなくてもよい。

サービスプロバイダ３－２の構成は、サービスプロバイダ３－１の構成と基本的に同様であるので、その図示および説明は省略する。

（５）ユーザホームネットワーク

（５－１）レシーバ５１

次に、図２６のブロック図を参照して、ユーザホームネットワーク５を構成するレシーバ５１の構成例を説明する。レシーバ５１は、通信部６１、ＳＡＭ６２、外部記憶部６３、伸張部６４、通信部６５、インタフェース６６、表示制御部６７、および入力制御部６８より構成されている。通信部６１は、ネットワーク４を介してサービスプロバイダ３、またはＥＭＤサービスセンタ１と通信し、所定の情報を受信し、または送信する。

ＳＡＭ６２は、相互認証モジュール７１、課金処理モジュール７２、記憶モジュール７３、復号／暗号化モジュール７４、およびデータ検査モジュール７５からなるが、シングルチップの暗号処理専用ＩＣで構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性（耐タンパー性）を有している。

ＳＡＭ６２の相互認証モジュール７１は、記憶モジュール７３に記憶されている、図２７に示すＳＡＭ６２の証明書を、相互認証相手に送信し、相互認証を実行し、これにより、認証相手と共有することとなった一時鍵Ｋｔｅｍｐ（セッション鍵）を復号／暗号化モジュール７４に供給する。ＳＡＭの証明書には、コン

テンツプロバイダ２－１の証明書（図１８）およびサービスプロバイダ３－１の証明書（図２５）に含まれている情報に対応する情報が含まれているので、その説明は省略する。

課金処理モジュール７２は、選択されたＵＣＰの利用内容に基づいて、使用許諾条件情報ＵＣＳおよび課金情報を作成する。図２８は、コンテンツが“買い取り再生”の利用形式で権利購入された場合のＵＣＳの例であり、図１２Ａに示したＵＣＰＡの利用内容１１と、図２０Ａに示したＰＴＡ－１に基づいて作成されたＵＣＳＡを表している。ＵＣＳには、図２８に示されるように、「コンテンツのＩＤ」、「コンテンツプロバイダのＩＤ」、「ＵＣＰのＩＤ」、「ＵＣＰの有効期限」、「サービスプロバイダのＩＤ」、「ＰＴのＩＤ」、「ＰＴの有効期限」、「ＵＣＳのＩＤ」、「ＳＡＭのＩＤ」、「ユーザのＩＤ」、「利用内容」、および「利用履歴」などの項目に設定される情報が含まれている。

ＵＣＳの、「コンテンツのＩＤ」、「コンテンツプロバイダのＩＤ」、「ＵＣＰのＩＤ」、「ＵＣＰの有効期限」、「サービスプロバイダのＩＤ」、「ＰＴのＩＤ」、および「ＰＴの有効期限」の各項目には、ＰＴの、それらに対応する項目の情報が設定される。すなわち、図２８のＵＣＳＡの、「コンテンツのＩＤ」には、コンテンツＡのＩＤが、「コンテンツプロバイダのＩＤ」には、コンテンツプロバイダ２－１のＩＤが、「ＵＣＰのＩＤ」には、ＵＣＰＡのＩＤが、「ＵＣＰの有効期限」には、ＵＣＰＡの有効期限が、「サービスプロバイダのＩＤ」には、サービスプロバイダ３－１のＩＤが、「ＰＴのＩＤ」には、ＰＴＡ－１のＩＤが、そして「ＰＴの有効期限」には、ＰＴＡ－１の有効期限が、それぞれ設定されている。

「ＵＣＳのＩＤ」には、ＵＣＳに割り当てられた所定のＩＤが設定され、ＵＣＳＡの「ＵＣＳのＩＤ」には、ＵＣＳＡのＩＤが設定されている。「ＳＡＭのＩＤ」には、機器のＳＡＭのＩＤが設定され、ＵＣＳＡの「ＳＡＭのＩＤ」には、レシーバ５１のＳＡＭ６２のＩＤが設定されている。「ユーザのＩＤ」には、コンテンツを利用するユーザのＩＤが設定され、ＵＣＳＡの「ユーザのＩＤ」には、ユーザＦのＩＤが設定されている。

「利用内容」は、「ＩＤ」、「形式」、「パラメータ」、および「管理移動状態情報」などの項目からなり、そのうち「ＩＤ」、「形式」、および「パラメータ」の項目には、選択されたＵＣＰの「利用内容」の、それらに対応する項目の情報が設定される。すなわち、ＵＣＳＡの「ＩＤ」には、ＵＣＰＡの「利用内容１１」の「ＩＤ１１」に設定されている情報（利用内容１１のＩＤ）が、「形式」には、「利用内容１１」の「形式１１」に設定されている”買い取り再生”が、「パラメータ」には、「利用内容１１」の「パラメータ１１」に設定されている情報（”買い取り再生”に対応する情報）が設定される。

「利用内容」の「管理移動状態情報」には、選択されたＵＣＰの「管理移動許可情報」に”可”が設定されている場合（管理移動が行える場合）、管理移動元の機器（コンテンツを購入した機器）と管理移動先の機器のそれぞれのＩＤが設定されるようになされている。なお、コンテンツの管理移動が行われていない状態においては、管理移動元の機器のＩＤと管理移動先の機器のＩＤは、共に、管理移動元の機器のＩＤとされる。一方、ＵＣＰの「管理移動許可情報」に、”不可”が設定されている場合、「管理移動状態情報」には、”不可”が設定される。すなわち、この場合、コンテンツの管理移動は行われない（許可されない）。ＵＣＳＡの「管理移動状態情報」には、ＵＣＰＡの「利用内容１１」の「管理移動許可情報１１」に”可”が設定されており、また、このとき、コンテンツＡは管理移動されていないので、ＳＡＭ６２のＩＤが、管理移動元の機器のＩＤおよび管理移動先の機器のＩＤとして設定されている。

「利用履歴」には、同一のコンテンツに対する利用履歴が含まれている。ＵＣＳＡの「利用履歴」には、”買い取り再生”を示す情報のみが記憶されているが、例えば、レシーバ５１において、コンテンツＡが以前に利用されていた場合、そのときの利用形式を示す情報も記憶されている。

なお、上述したＵＣＳにおいては、「ＵＣＰの有効期限」および「ＰＴの有効期限」が設けられているがそれらをＵＣＳに設定しないようにすることもできる。また、上述したＵＣＳにおいて、「コンテンツプロバイダのＩＤ」が設けられてい

るが、ＵＣＰのＩＤがユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダのＩＤ」も同様に、ＰＴのＩＤがユニークで、これにより、サービスプロバイダを特定することができる場合、それを設けないようにすることもできる。

作成されたＵＣＳは、レシーバ５１の復号／暗号化モジュール７４の復号化ユニット９１から供給されるコンテンツ鍵Ｋｃｏ（保存用鍵Ｋｓａｖｅで暗号化されている）とともに、外部記憶部６３に送信され、その利用情報記憶部６３Ａに記憶される。外部記憶部６３の利用情報記憶部６３Ａは、図２９に示すように、Ｍ個のブロックＢＰ－１乃至ＢＰ－Ｍに分割され（例えば、１メガバイト毎に分割され)、各ブロックＢＰが、Ｎ個の利用情報用メモリ領域ＲＰ－１乃至ＲＰ－Ｎに分割されている。ＳＡＭ６２から供給されるコンテンツ鍵Ｋｃｏ（保存用鍵Ｋｓａｖｅで暗号化されている）およびＵＣＳは、利用情報用記憶部６３Ａの所定のブロックＢＰの利用情報用メモリ領域ＲＰに、対応して記憶される。

図２９の例では、ブロックＢＰ－１の利用情報用メモリ領域ＲＰ－３に、図２８に示したＵＣＳＡと、コンテンツＡを復号するためのコンテンツ鍵ＫｃｏＡ（保存用鍵Ｋｓａｖｅで暗号化されている）が対応して記憶されている。ブロックＢＰ－１の利用情報用メモリ領域ＲＰ－１，ＲＰ－２には、他のコンテンツ鍵Ｋｃｏ１，Ｋｃｏ２（それぞれ保存用鍵Ｋｓａｖｅで暗号化されている）およびＵＣＳ１，２がそれぞれ記憶されている。ブロックＢＰ－１の利用情報用メモリ領域ＲＰ－４（図示せず）乃至ＲＰ－Ｎ、およびブロックＢＰ－２（図示せず）乃至ＢＰ－Ｍには、コンテンツ鍵ＫｃｏおよびＵＣＳは記憶されておらず、空いていることを示す所定の初期情報が記憶されている。なお、利用情報用メモリ領域ＲＰに記憶されるコンテンツ鍵Ｋｃｏ（保存用鍵Ｋｓａｖｅで暗号化されている）およびＵＣＳを、個々に区別する必要がない場合、まとめて、利用情報と称する。

図３０は、図２８に示したＵＣＳＡと同時に作成された課金情報Ａを表してい

る。課金情報には、図３０に示されるように、「コンテンツのＩＤ」、「コンテンツプロバイダのＩＤ」、「ＵＣＰのＩＤ」、「ＵＣＰの有効期限」、「サービスプロバイダのＩＤ」、「ＰＴのＩＤ」、「ＰＴの有効期限」、「ＵＣＳのＩＤ」、「ＳＡＭのＩＤ」、「ユーザのＩＤ」、「利用内容」、および「課金履歴」などの項目に設定される情報が含まれている。

課金情報の、「コンテンツのＩＤ」、「コンテンツプロバイダのＩＤ」、「ＵＣＰのＩＤ」、「ＵＣＰの有効期限」、「サービスプロバイダのＩＤ」、「ＰＴのＩＤ」、「ＰＴの有効期限」、「ＵＣＳのＩＤ」、「ＳＡＭのＩＤ」、「ユーザのＩＤ」、および「利用内容」には、ＵＣＳの、それらに対応する項目の情報が、それぞれ設定されている。すなわち、図３０の課金情報Ａの、「コンテンツのＩＤ」には、コンテンツＡのＩＤが、「コンテンツプロバイダのＩＤ」には、コンテンツプロバイダ２－１のＩＤが、「ＵＣＰのＩＤ」には、ＵＣＰＡのＩＤが、「ＵＣＰの有効期限」には、ＵＣＰＡの有効期限が、「サービスプロバイダのＩＤ」には、サービスプロバイダ３－１のＩＤが、「ＰＴのＩＤ」には、ＰＴＡ－１のＩＤが、「ＰＴの有効期限」には、ＰＴＡ－１の有効期限が、「ＵＣＳのＩＤ」には、ＵＣＳＡのＩＤが、「ＳＡＭのＩＤ」には、ＳＡＭ６２のＩＤが、「ユーザのＩＤ」には、ユーザＦのＩＤが、そして「利用内容」には、ＵＣＳＡの「利用内容１１」の内容が、それぞれ設定されている。

課金情報の「課金履歴」には、機器において計上された課金の合計額を示す情報などが設定される。課金情報Ａの「課金履歴」には、レシーバ５１において計上された課金の合計額が設定されている。

なお、上述した課金情報においては、「ＵＣＰの有効期限」および「ＰＴの有効期限」が設けられているがそれらをＵＣＳに設定しないようにすることもできる。また、上述した課金情報において、「コンテンツプロバイダのＩＤ」が設けられているが、ＵＣＰのＩＤがユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダのＩＤ」も同様に、ＰＴのＩＤがユニークで、これにより、サー

ビスプロバイダを特定することができる場合、それを設けないようにすることもできる。

図２６に戻り、記憶モジュール７３には、図３１に示すように、ＳＡＭ６２の公開鍵Ｋｐｕ、ＳＡＭ６２の秘密鍵Ｋｓｕ、ＥＭＤサービスセンタ１の公開鍵Ｋｐｅｓｃ、認証局の公開鍵Ｋｐｃａ、保存用鍵Ｋｓａｖｅ、３ヶ月分の配送用鍵Ｋｄなどの各種鍵、ＳＡＭ６２の証明書（図２７）、課金情報（例えば、図３０の課金情報Ａなど）、基準情報５１、およびＭ個の検査値ＨＰ－１乃至ＨＰ－Ｍなどが記憶されている。

図３２は、記憶モジュール７３に記憶されている基準情報５１を表している。基準情報には、「ＳＡＭのＩＤ」、「機器番号」、「決済ＩＤ」、「課金の上限額」、「決済ユーザ情報」、「従属ユーザ情報」、および「利用ポイント情報」の各項目に設定される所定の情報などが含まれている。

基準情報の、「ＳＡＭのＩＤ」、「機器番号」、「決済ＩＤ」、「決済ユーザ情報」、「従属ユーザ情報」、および「利用ポイント情報」の項目には、ＥＭＤサービスセンタ１のユーザ管理部１８により管理されるシステム登録情報（図９）の、それらに対応する項目の情報が設定される。すなわち、基準情報５１には、ＳＡＭ６２のＩＤ、ＳＡＭ６２の機器番号（１００番）、ユーザＦの決済ＩＤ、ユーザＦの決済ユーザ情報（ユーザＦのユーザ一般情報（氏名、住所、電話番号、決済機関情報、生年月日、年齢、性別）、ユーザＦのＩＤ、およびユーザＦのパスワード）、および図３３に示す利用ポイント情報（図１０Ａ）に示したものと同様の情報）が設定されている。

「課金の上限額」には、機器がＥＭＤシステムに正式登録されている状態と仮登録されている状態で、それぞれ異なる額が、課金の上限額として設定される。基準情報５１の「課金の上限額」には、レシーバ５１が正式登録されているので、正式登録されている状態における課金の上限額”正式登録時の上限額 ”）が設定されている。なお、正式登録されている状態における課金の上限額は、仮登録されている状態における課金の上限額よりも、大きな額である。

次に、記憶モジュール７３に記憶される、図３１に示したM個の検査値ＨＰ－１乃至ＨＰ－Mについて説明する。検査値ＨＰ－１は、外部記憶部６３の利用情報記憶部６３Ａ（図２９）のブロックＢＰ－１に記憶されているデータの全体にハッシュ関数が適用されて算出されたハッシュ値である。検査値ＨＰ－２乃至ＨＰ－Mも、検査値ＨＰ－１と同様に、外部記憶部６３の、対応するブロックＢＰ－２乃至ＢＰ－Mのそれぞれに記憶されているデータのハッシュ値である。

図２６に戻り、ＳＡＭ６２の復号／暗号化モジュール７４は、復号ユニット９１、乱数発生ユニット９２、および暗号化ユニット９３から構成される。復号ユニット９１は、暗号化されたコンテンツ鍵Ｋｃｏを配送用鍵Ｋｄで復号し、暗号化ユニット９３に出力する。乱数発生ユニット９２は、必要に応じて（例えば、相互認証時）、所定の桁数の乱数を発生して一時鍵Ｋｔｅｍｐを生成し、暗号化ユニット９３に出力する。

暗号化ユニット９３は、復号されたコンテンツ鍵Ｋｃｏを、再度、記憶モジュール７３に保持されている保存用鍵Ｋｓａｖｅで暗号化する。暗号化されたコンテンツ鍵Ｋｃｏは、外部記憶部６３に供給される。暗号化ユニット９３は、コンテンツ鍵Ｋｃｏを伸張部６４に送信するとき、コンテンツ鍵Ｋｃｏを乱数発生ユニット９２で生成した一時鍵Ｋｔｅｍｐで暗号化する。

データ検査モジュール７５は、記憶モジュール７３に記憶されている検査値ＨＰと、外部記憶部６３の利用情報記憶部６３Ａの、対応するブロックＢＰのデータのハッシュ値を比較し、ブロックＢＰのデータが改竄されていないか否かを検査する。データ検査モジュー７５はまた、コンテンツの購入、移動、および管理移動等が行われる際に、検査値ＨＰを再算出し、記憶モジュール７３に記憶（更新）させる。

伸張部６４は、相互認証モジュール１０１、復号モジュール１０２、復号モジュール１０３、伸張モジュール１０４、およびウォータマーク付加モジュール１０５から構成される。相互認証モジュール１０１は、ＳＡＭ６２と相互認証し、一時鍵Ｋｔｅｍｐを復号モジュール１０２に出力する。復号モジュール１０２は

、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵Ｋｃｏを一時鍵Ｋｔｅｍｐで復号し、復号モジュール１０３に出力する。復号モジュール１０３は、ＨＤＤ５２に記録されたコンテンツをコンテンツ鍵Ｋｃｏで復号し、伸張モジュール１０４に出力する。伸張モジュール１０４は、復号されたコンテンツを、更にＡＴＲＡＣ２等の方式で伸張し、ウォータマーク付加モジュール１０５に出力する。ウォータマーク付加モジュール１０５は、コンテンツにレシーバ５１を特定するための情報（例えば、ＳＡＭ６２のＩＤ）のウォータマーク（電子透かし）を挿入し、図示せぬスピーカに出力し、音楽を再生する。

通信部６５は、ユーザホームネットワーク５のレシーバ２０１との通信処理を行う。インターフェース６６は、ＳＡＭ６２および伸張部６４からの信号を所定の形式に変更し、ＨＤＤ５２に出力し、また、ＨＤＤ５２からの信号を所定の形式に変更し、ＳＡＭ６２および伸張部６４に出力する。

表示制御部６７は、表示部（図示せず）への出力を制御する。入力制御部６８は、各種ボタンなどから構成される操作部（図示せず）からの入力を制御する。

ＨＤＤ５２は、サービスプロバイダ３から供給されたコンテンツ、ＵＣＰ、およびＰＴの他、図３４に示すような、登録リストを記憶している。この登録リストは、表形式に情報が記憶されているリスト部、および登録リストを保持する機器についての所定の情報が記憶されている対象ＳＡＭ情報部より構成されている。

対象ＳＡＭ情報部には、この登録リストを保有する機器のＳＡＭＩＤ、この例の場合、レシーバ５１のＳＡＭ６２のＩＤが（「対象ＳＡＭＩＤ」の欄に）記憶されている。対象ＳＡＭ情報部にはまた、この登録リストの有効期限が（「有効期限」の欄に）記憶され、登録リストのバージョン番号が（「バージョン番号」の欄に）記憶され、そして接続されている機器の数（自分自身を含む）、この例の場合、レシーバ５１には、他の機器が接続されていないので、自分自身を含む値１が（「接続されている機器数」の欄に）記憶されている。

リスト部は、「ＳＡＭ　ＩＤ」、「ユーザＩＤ」、「購入処理」、「課金処理」、「課

金機器」、「コンテンツ供給機器」、「状態フラグ」、「登録条件署名」、および「登録リスト署名」の９個の項目から構成され、この例の場合、レシーバ５１の登録条件として、それぞれの項目に所定の情報が記憶されている。

「ＳＡＭ　ＩＤ」には、機器のＳＡＭのＩＤが記憶される。この例の場合、レシーバ５１のＳＡＭ６２のＩＤが記憶されている。「ユーザＩＤ」には、対応する機器のユーザのＩＤが記憶される。この例の場合、ユーザＦのＩＤが記憶されている。

「購入処理」には、コンテンツを購入するための処理を行うことができるか否かを示す情報（”可”または”不可”）が記憶される。この例の場合、レシーバ５１は、コンテンツを購入するための処理を行うことができるので、”可”が記憶されている。

「課金処理」には、ＥＭＤサービスセンタ１との間で、課金を決済する処理を行うことができるか否かを示す情報（”可”または”不可”）が記憶される。この例の場合、レシーバ５１は、ユーザＦが決済ユーザとして登録されているので、課金を決済する処理を行うことができる。そのため、「課金処理」には、”可”が記憶されている。

「課金機器」には、計上された課金に対する課金処理を行う機器のＳＡＭのＩＤが記憶される。この例の場合、レシーバ５１（ＳＡＭ６２）は、自分自身が、課金を決済することができるので、ＳＡＭ６２のＩＤが記憶されている。

「コンテンツ供給機器」には、対応する機器が、コンテンツの供給をサービスプロバイダ３からではなく、接続される他の機器から受ける場合、コンテンツを供給することができる機器のＳＡＭのＩＤが記憶される。この例の場合、レシーバ５１は、コンテンツの供給をサービスプロバイダ３から受けるので、コンテンツを供給する機器が存在しない旨を示す情報（”なし”）が記憶されている。

「状態フラグ」には、対応する機器の動作制限条件が記憶される。何ら制限されていない場合は、その旨を示す情報（”制限なし”）、一定の制限が課せられている場合は、その旨を示す情報（”制限あり”）、また動作が停止させられている

場合には、その旨を示す情報（”停止”）が記憶される。例えば、決済が成功しなかった場合や、正式登録されるための与信処理が完了していない場合（仮登録されている場合）、「状態フラグ」には、”制限あり ”が設定される。この例の場合、「状態フラグ」に”制限あり ”が設定された機器においては、すでに購入されたコンテンツを利用する処理は実行されるが、新たなコンテンツを購入するための処理は実行されなくなる。すなわち、一定の制限が機器に課せられる。また、コンテンツの不正複製などの違反行為が発覚した場合、「状態フラグ」には、”停止”が設定され、機器の動作が停止される。これにより、その機器はＥＭＤシステムからのサービスを、一切受けることができなくなる。

この例の場合、レシーバ５１に対しては、何ら制限が課せられていないものとし、「状態フラグ」には”なし”が設定されている。

「登録条件署名」には、登録条件として、それぞれ、「ＳＡＭ　ＩＤ」、「ユーザＩＤ」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、および「状態フラグ」に記憶されている情報に対するＥＭＤサービスセンタ１による署名が記憶されている。この例の場合、レシーバ５１の登録条件に対する署名が記憶されている。「登録リスト署名」には、登録リストに設定されたデータの全体に対する署名が設定されている。

（５－２）レシーバ２０１

図３５は、レシーバ２０１の構成例を表している。レシーバ２０１の通信部２１１乃至入力制御部２１８は、レシーバ５１の通信部６１乃至入力制御部６８と同様の機能を有しているので、その説明は適宜省略する。

ＳＡＭ２１２の記憶モジュール２２３にも、図３６に示すように、ＳＡＭ２１２の公開鍵Ｋｐｕ、ＳＡＭ２１２の秘密鍵Ｋｓｕ、ＥＭＤサービスセンタ１の公開鍵Ｋｐｅｓｃ、認証局の公開鍵Ｋｐｃａ、保存用鍵Ｋｓａｖｅ、３月分の配送用鍵Ｋｄ、予め認証局から配布されているＳＡＭ２１２の証明書、および基準情報２０１が記憶されている。基準情報２０１には、図３７に示すように、ＳＡＭ２１２のＩＤ、レシーバ２０１の機器番号（１００番）、ユーザＡの決済ＩＤ、ユ

ーザＡの決済ユーザ情報（ユーザＡのユーザー般情報（氏名、住所、電話番号、決済機関情報、生年月日、年齢、性別）、ユーザＡのＩＤ、およびユーザＡのパスワード）、および図３８に示す利用ポイント情報（図１０Ｂに示したものと同様の情報）が設定されている。

ＨＤＤ２０２は、ＨＤＤ５２と同様の機能を有するので、その説明は省略する。

（６）コンテンツの購入及び利用

次に、ＥＭＤシステムの処理について、図３９のフローチャートを参照して説明するが、ここでは、コンテンツプロバイダ２－１に保持されているコンテンツＡが、サービスプロバイダ３－１を介して、ユーザホームネットワーク５のレシーバ５１に供給され、利用される場合を例として説明する。

（６－１）ＥＭＤサービスセンタからコンテンツプロバイダへの配送用鍵の伝送

ステップＳ１１において、配送用鍵Ｋｄが、ＥＭＤサービスセンタ１からコンテンツプロバイダ２－１に供給される処理が行われる。この処理の詳細は、図４０のフローチャートに示されている。すなわち、ステップＳ３１において、ＥＭＤサービスセンタ１の相互認証部１７は、コンテンツプロバイダ２－１の相互認証部３９と相互認証し、コンテンツプロバイダ２－１が、正当なプロバイダであることが確認した後、ＥＭＤサービスセンタ１のコンテンツプロバイダ管理部１２は、鍵サーバ１４から供給された配送用鍵Ｋｄをコンテンツプロバイダ２－１に送信する。なお、相互認証処理の詳細は、図４１乃至図４３を参照して後述する。

次に、ステップＳ３２において、コンテンツプロバイダ２－１の暗号化部３６は、ＥＭＤサービスセンタ１から送信された配送用鍵Ｋｄを受信し、ステップＳ３３において、記憶する。

このように、コンテンツプロバイダ２－１の暗号化部３６が、配送用鍵Ｋｄを記憶したとき、処理は終了し、図３９のステップＳ１２に進む。ここで、ステップＳ１２以降の処理の説明の前に、図４０のステップＳ３１における相互認証処

理（なりすましがないことを確認する処理）について、１つの共通鍵を用いる場合（図４１）、２つの共通鍵を用いる場合（図４２）、および公開鍵暗号を用いる場合（図４３）を例として説明する。

図４１は、１つの共通鍵で、共通鍵暗号であるＤＥＳを用いる、コンテンツプロバイダ２の相互認証部３９とＥＭＤサービスセンタ１の相互認証部１７との相互認証の動作を説明するフローチャートである。ステップＳ４１において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ１を生成する（乱数生成部３５が生成するようにしてもよい）。ステップＳ４２において、コンテンツプロバイダ２の相互認証部３９は、ＤＥＳを用いて乱数Ｒ１を、予め記憶している共通鍵Ｋｃで暗号化する（暗号化部３６で暗号化するようにしてもよい）。ステップＳ４３において、コンテンツプロバイダ２の相互認証部３９は、暗号化された乱数Ｒ１をＥＭＤサービスセンタ１の相互認証部１７に送信する。

ステップＳ４４において、ＥＭＤサービスセンタ１の相互認証部１７は、受信した乱数Ｒ１を予め記憶している共通鍵Ｋｃで復号する。ステップＳ４５において、ＥＭＤサービスセンタ１の相互認証部１７は、３２ビットの乱数Ｒ２を生成する。ステップＳ４６において、ＥＭＤサービスセンタ１の相互認証部１７は、復号した６４ビットの乱数Ｒ１の下位３２ビットを乱数Ｒ２で入れ替え、連接$R1_H \| R2$を生成する。なお、ここでRi_Hは、Ｒｉの上位ｎビットを表し、Ａ‖Ｂは、ＡとＢの連接（ｎビットのＡの下位に、ｍビットのＢを結合して、（ｎ＋ｍ）ビットとしたもの）を表す。ステップＳ４７において、ＥＭＤサービスセンタ１の相互認証部１７は、ＤＥＳを用いて$R1_H \| R2$を共通鍵Ｋｃで暗号化する。ステップＳ４８において、ＥＭＤサービスセンタ１の相互認証部１７は、暗号化した$R1_H \| R2$をコンテンツプロバイダ２に送信する。

ステップＳ４９において、コンテンツプロバイダ２の相互認証部３９は、受信した$R1_H \| R2$を共通鍵Ｋｃで復号する。ステップＳ５０において、コンテンツプロバイダ２の相互認証部３９は、復号した$R1_H \| R2$の上位３２ビット$R1_H$を調べ、ステップＳ４１で生成した、乱数Ｒ１の上位３２ビット$R1_H$と一致す

れば、ＥＭＤサービスセンタ１が正当なセンタであることを認証する。生成した乱数$R1_H$と、受信した$R1_H$が一致しないとき、処理は終了される。両者が一致するとき、ステップＳ５１において、コンテンツプロバイダ２の相互認証部３９は、３２ビットの乱数Ｒ３を生成する。ステップＳ５２において、コンテンツプロバイダ２の相互認証部３９は、受信して復号した$R1_H \| R2$から下位３２ビットを取り出した乱数Ｒ２を上位に設定し、生成した乱数Ｒ３をその下位に設定し、連接Ｒ２‖Ｒ３とする。ステップＳ５３において、コンテンツプロバイダ２の相互認証部３９は、ＤＥＳを用いて連接Ｒ２‖Ｒ３を共通鍵Ｋｃで暗号化する。ステップＳ５４において、コンテンツプロバイダ２の相互認証部３９は、暗号化された連接Ｒ２‖Ｒ３をＥＭＤサービスセンタ１の相互認証部１７に送信する。

ステップＳ５５において、ＥＭＤサービスセンタ１の相互認証部１７は、受信した連接Ｒ２‖Ｒ３を共通鍵Ｋｃで復号する。ステップＳ５６において、ＥＭＤサービスセンタ１の相互認証部１７は、復号した連接Ｒ２‖Ｒ３の上位３２ビットを調べ、乱数Ｒ２と一致すれば、コンテンツプロバイダ２を正当なプロバイダとして認証し、一致しなければ、不正なプロバイダとして、処理を終了する。

図４２は、２つの共通鍵Ｋｃ１，Ｋｃ２で、共通鍵暗号であるＤＥＳを用いる、コンテンツプロバイダ２の相互認証部３９とＥＭＤサービスセンタ１の相互認証部１７との相互認証の動作を説明するフローチャートである。ステップＳ６１において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ１を生成する。ステップＳ６２において、コンテンツプロバイダ２の相互認証部３９は、ＤＥＳを用いて乱数Ｒ１を予め記憶している共通鍵Ｋｃ１で暗号化する。ステップＳ６３において、コンテンツプロバイダ２の相互認証部３９は、暗号化された乱数Ｒ１をＥＭＤサービスセンタ１に送信する。

ステップＳ６４において、ＥＭＤサービスセンタ１の相互認証部１７は、受信した乱数Ｒ１を予め記憶している共通鍵Ｋｃ１で復号する。ステップＳ６５において、ＥＭＤサービスセンタ１の相互認証部１７は、乱数Ｒ１を予め記憶してい

る共通鍵Ｋｃ２で暗号化する。ステップＳ６６において、ＥＭＤサービスセンタ１の相互認証部１７は、６４ビットの乱数Ｒ２を生成する。ステップＳ６７において、ＥＭＤサービスセンタ１の相互認証部１７は、乱数Ｒ２を共通鍵Ｋｃ２で暗号化する。ステップＳ６８において、ＥＭＤサービスセンタ１の相互認証部１７は、暗号化された乱数Ｒ１および乱数Ｒ２をコンテンツプロバイダ２の相互認証部３９に送信する。

ステップＳ６９において、コンテンツプロバイダ２の相互認証部３９は、受信した乱数Ｒ１および乱数Ｒ２を予め記憶している共通鍵Ｋｃ２で復号する。ステップＳ７０において、コンテンツプロバイダ２の相互認証部３９は、復号した乱数Ｒ１を調べ、ステップＳ６１で生成した乱数Ｒ１（暗号化する前の乱数Ｒ１）と一致すれば、ＥＭＤサービスセンタ１を適正なセンタとして認証し、一致しなければ、不正なセンタであるとして、処理を終了する。ステップＳ７１において、コンテンツプロバイダ２の相互認証部３９は、復号して得た乱数Ｒ２を共通鍵Ｋｃ１で暗号化する。ステップＳ７２において、コンテンツプロバイダ２の相互認証部３９は、暗号化された乱数Ｒ２をＥＭＤサービスセンタ１に送信する。

ステップＳ７３において、ＥＭＤサービスセンタ１の相互認証部１７は、受信した乱数Ｒ２を共通鍵Ｋｃ１で復号する。ステップＳ７４において、ＥＭＤサービスセンタ１の相互認証部１７は、復号した乱数Ｒ２が、ステップＳ６６で生成した乱数Ｒ２（暗号化する前の乱数Ｒ２）と一致すれば、コンテンツプロバイダ２を適正なプロバイダとして認証し、一致しなければ、不正なプロバイダであるとして処理を終了する。

図４３は、公開鍵暗号である、１６０ビット長の楕円曲線暗号を用いる、コンテンツプロバイダ２の相互認証部３９とＥＭＤサービスセンタ１の相互認証部１７との相互認証の動作を説明するフローチャートである。ステップＳ８１において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ１を生成する。ステップＳ８２において、コンテンツプロバイダ２の相互認証部３９は、自分自身の公開鍵Ｋｐｃｐを含む証明書（認証局から予め取得しておいたもの）

と、乱数Ｒ１をＥＭＤサービスセンタ１の相互認証部１７に送信する。

ステップＳ８３において、ＥＭＤサービスセンタ１の相互認証部１７は、受信した証明書の署名（認証局の秘密鍵Ｋｓｃａで暗号化されている）を、予め取得しておいた認証局の公開鍵Ｋｐｃａで復号し、コンテンツプロバイダ２の公開鍵Ｋｐｃｐとコンテンツプロバイダ２の名前のハッシュ値を取り出すとともに、証明書に平文のまま格納されているコンテンツプロバイダ２の公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前を取り出す。証明書が認証局が発行した適正なものであれば、証明書の署名を復号することが可能であり、復号して得られた公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前のハッシュ値は、平文のまま証明書に格納されていたコンテンツプロバイダ２の公開鍵Ｋｐｃｐおよびコンテンツプロバイダ２の名前にハッシュ関数を適用して得られたハッシュ値と一致する。これにより、公開鍵Ｋｐｃｐが改竄されたものでない適正なものであることが認証される。署名を復号出来なかったり、できたとしてもハッシュ値が一致しないときには、適正な公開鍵でないか、適正なプロバイダでないことになる。この時処理は終了される。

適正な認証結果が得られたとき、ステップＳ８４において、ＥＭＤサービスセンタ１の相互認証部１７は、６４ビットの乱数Ｒ２を生成する。ステップＳ８５において、ＥＭＤサービスセンタ１の相互認証部１７は、乱数Ｒ１および乱数Ｒ２の連接Ｒ１‖Ｒ２を生成する。ステップＳ８６において、ＥＭＤサービスセンタ１の相互認証部１７は、連接Ｒ１‖Ｒ２を自分自身の秘密鍵Ｋｓｅｓｃで暗号化する。ステップＳ８７において、ＥＭＤサービスセンタ１の相互認証部１７は、連接Ｒ１‖Ｒ２を、ステップＳ８３で取得したコンテンツプロバイダ２の公開鍵Ｋｐｃｐで暗号化する。ステップＳ８８において、ＥＭＤサービスセンタ１の相互認証部１７は、秘密鍵Ｋｓｅｓｃで暗号化された連接Ｒ１‖Ｒ２、公開鍵Ｋｐｃｐで暗号化された連接Ｒ１‖Ｒ２、および自分自身の公開鍵Ｋｐｅｓｃを含む証明書（認証局から予め取得しておいたもの）をコンテンツプロバイダ２の相互認証部３９に送信する。

ステップＳ８９において、コンテンツプロバイダ２の相互認証部３９は、受信した証明書の署名を予め取得しておいた認証局の公開鍵Ｋｐｃａで復号し、正しければ証明書から公開鍵Ｋｐｅｓｃを取り出す。この場合の処理は、ステップＳ８３における場合と同様であるので、その説明は省略する。ステップＳ９０において、コンテンツプロバイダ２の相互認証部３９は、ＥＭＤサービスセンタ１の秘密鍵Ｋｓｅｓｃで暗号化されている連接Ｒ１‖Ｒ２を、ステップＳ８９で取得した公開鍵Ｋｐｅｓｃで復号する。ステップＳ９１において、コンテンツプロバイダ２の相互認証部３９は、自分自身の公開鍵Ｋｐｃｐで暗号化されている連接Ｒ１‖Ｒ２を、自分自身の秘密鍵Ｋｓｃｐで復号する。ステップＳ９２において、コンテンツプロバイダ２の相互認証部３９は、ステップＳ９０で復号された連接Ｒ１‖Ｒ２と、ステップＳ９１で復号された連接Ｒ１‖Ｒ２を比較し、一致すればＥＭＤサービスセンタ１を適正なものとして認証し、一致しなければ、不適正なものとして、処理を終了する。

適正な認証結果が得られたとき、ステップＳ９３において、コンテンツプロバイダ２の相互認証部３９は、６４ビットの乱数Ｒ３を生成する。ステップＳ９４において、コンテンツプロバイダ２の相互認証部３９は、ステップＳ９０で取得した乱数Ｒ２および生成した乱数Ｒ３の連接Ｒ２‖Ｒ３を生成する。ステップＳ９５において、コンテンツプロバイダ２の相互認証部３９は、連接Ｒ２‖Ｒ３を、ステップＳ８９で取得した公開鍵Ｋｐｅｓｃで暗号化する。ステップＳ９６において、コンテンツプロバイダ２の相互認証部３９は、暗号化した連接Ｒ２‖Ｒ３をＥＭＤサービスセンタ１の相互認証部１７に送信する。

ステップＳ９７において、ＥＭＤサービスセンタ１の相互認証部１７は、暗号化された連接Ｒ２‖Ｒ３を自分自身の秘密鍵Ｋｓｅｓｃで復号する。ステップＳ９８において、ＥＭＤサービスセンタ１の相互認証部１７は、復号した乱数Ｒ２が、ステップＳ８４で生成した乱数Ｒ２（暗号化する前の乱数Ｒ２）と一致すれば、コンテンツプロバイダ２を適正なプロバイダとして認証し、一致しなけば、不適正なプロバイダとして、処理を終了する。

以上のように、ＥＭＤサービスセンタ１の相互認証部１７とコンテンツプロバイダ２の相互認証部３９は、相互認証する。相互認証に利用された乱数は、その相互認証に続く処理にだけ有効な一時鍵Ｋｔｅｍｐとして利用される。

（６－２）コンテンツプロバイダからサービスプロバイダへのコンテンツの伝送

次に、図３９のステップＳ１２の処理について説明する。ステップＳ１２においては、コンテンツプロバイダセキュアコンテナが、コンテンツプロバイダ２－１からサービスプロバイダ３－１に供給される処理が行われる。その処理の詳細は、図４４のフローチャートに示されている。すなわち、ステップＳ２０１において、コンテンツプロバイダ２－１のウォータマーク付加部３２は、コンテンツサーバ３１からコンテンツＡを読み出し、コンテンツプロバイダ２－１を示す所定のウォータマーク（電子透かし）を挿入し、圧縮部３３に供給する。

ステップＳ２０２において、コンテンツプロバイダ２－１の圧縮部３３は、ウォータマークが挿入されたコンテンツＡをＡＴＲＡＣ２等の所定の方式で圧縮し、暗号化部３４に供給する。ステップＳ２０３において、乱数発生部３５は、コンテンツ鍵ＫｃｏＡとなる乱数を発生させ、暗号化部３４に供給する。

ステップＳ２０４において、コンテンツプロバイダ２－１の暗号化部３４は、ＤＥＳなどの所定の方式で、乱数発生部３５で発生された乱数（コンテンツ鍵ＫｃｏＡ）を使用して、ウォータマークが挿入されて圧縮されたコンテンツＡを暗号化する。次に、ステップＳ２０５において、暗号化部３６は、ＤＥＳなどの所定の方式で、ＥＭＤサービスセンタ１から供給された配送用鍵Ｋｄでコンテンツ鍵ＫｃｏＡを暗号化する。

ステップＳ２０６において、コンテンツプロバイダ２－１のセキュアコンテナ作成部３８は、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、およびポリシー記憶部３７に記憶されている、コンテンツＡに対応するＵＣＰＡ，Ｂ（図１２）の全体にハッシュ関数を適用してハッシュ値を算出し、自分自身の秘密鍵Ｋｓｃｐで暗号化する。これにより、図１７に示した署名が作成される。

ステップＳ２０７において、コンテンツプロバイダ２－１のセキュアコンテナ作成部３８は、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、ＵＣＰＡ，Ｂ（図１２）、およびステップＳ２０６で生成した署名を含んだ、図１７に示したコンテンツプロバイダセキュアコンテナを作成する。

ステップＳ２０８において、コンテンツプロバイダ２－１の相互認証部３９は、サービスプロバイダ３－１の相互認証部４５と相互認証する。この認証処理は、図４１乃至図４３を参照して説明した場合と同様であるので、その説明は省略する。ステップＳ２０９において、コンテンツプロバイダ２－１のセキュアコンテナ作成部３８は、認証局から予め発行された証明書（図１８）を、ステップＳ２０７で作成したコンテンツプロバイダセキュアコンテナに付して、サービスプロバイダ３－１に送信する。

このようにして、コンテンツプロバイダセキュアコンテナが、サービスプロバイダ３－１に供給されたとき、処理は終了し、図３９のステップＳ１３に進む。

（６－３）サービスプロバイダからレシーバへのコンテンツの伝送

ステップＳ１３において、サービスプロバイダセキュアコンテナが、サービスプロバイダ３－１からユーザホームネットワーク５（レシーバ５１）に供給される。この処理の詳細は、図４５のフローチャートに示されている。すなわち、ステップＳ２２１において、サービスプロバイダ３－１の値付け部４２は、コンテンツプロバイダ２－１から送信されたコンテンツプロバイダセキュアコンテナに付された証明書（図１８）に含まれる署名を確認し、証明書の改竄がなければ、それから、コンテンツプロバイダ２－１の公開鍵Ｋｐｃｐを取り出す。証明書の署名の確認は、図４３のステップＳ８３における処理と同様であるので、その説明は省略する。

ステップＳ２２２において、サービスプロバイダ３－１の値付け部４２は、コンテンツプロバイダ２－１から送信されたコンテンツプロバイダセキュアコンテナの署名をコンテンツプロバイダ２－１の公開鍵Ｋｐｃｐで復号し、得られたハ

ッシュ値が、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、およびＵＣＰＡ，Ｂの全体にハッシュ関数を適用して得られたハッシュ値と一致するか否かを判定し、コンテンツプロバイダセキュアコンテナの改竄がないことを確認する。両者の値が一致しない場合（改竄が発見された場合）は、処理は終了されるが、この例の場合、コンテンツプロバイダセキュアコンテナの改竄はなかったものとし、ステップＳ２２３に進む。

ステップＳ２２３において、サービスプロバイダ３－１の値付け部４２は、コンテンツプロバイダセキュアコンテナから、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、および署名を取り出し、コンテンツサーバ４１に供給する。コンテンツサーバ４１は、それらを記憶する。値付け部４２はまたＵＣＰＡ，Ｂも、コンテンツプロバイダセキュアコンテナから取り出し、セキュアコンテナ作成部４４に供給する。

ステップＳ２２４において、サービスプロバイダ３－１の値付け部４２は、取り出したＵＣＰＡ，Ｂに基づいて、ＰＴＡ－１，Ａ－２（図２０）、およびＰＴＢ－１，Ｂ－２（図２２）を作成し、セキュアコンテナ作成部４４に供給する。

ステップＳ２２５において、サービスプロバイダ３－１のセキュアコンテナ作成部４４は、コンテンツサーバ４１から読み出したコンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、コンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）、およびコンテンツプロバイダ２の署名、値付け部４２から供給された、ＵＣＰＡ，Ｂ、およびＰＴＡ－１，Ａ－２，Ｂ－１，Ｂ－２、並びにその署名から、図２４に示したサービスプロバイダセキュアコンテナを作成する。

ステップＳ２２６において、サービスプロバイダ３－１の相互認証部４５は、レシーバ５１の相互認証モジュール７１と相互認証する。この認証処理は、図４１乃至図４３を参照して説明した場合と同様であるので、その説明を省略する。

ステップＳ２２７において、サービスプロバイダ３－１のセキュアコンテナ作

成部４４は、ステップＳ２２５で作成したサービスプロバイダセキュアコンテナに、サービスプロバイダ３－１の証明書（図２５）を付して、ユーザホームネットワーク５のレシーバ５１に送信する。

このようにして、サービスプロバイダセキュアコンテナが、サービスプロバイダ３－１からレシーバ５１に送信されたとき、処理は終了し、図３９のステップＳ１４に進む。

（６－４）レシーバによるコンテンツの記録処理

ステップＳ１４において、サービスプロバイダ３－１から送信されたサービスプロバイダセキュアコンテナが、ユーザホームネットワーク５のレシーバ５１により受信される。この処理の詳細は、図４６のフローチャートに示されている。すなわち、ステップＳ２４１において、レシーバ５１の相互認証モジュール７１は、通信部６１を介して、サービスプロバイダ３－１の相互認証部４５と相互認証し、相互認証できたとき、通信部６１は、相互認証したサービスプロバイダ３－１から、サービスプロバイダセキュアコンテナ（図２４）を受信する。相互認証できなかった場合、処理は終了されるが、この例の場合、相互認証されたものとし、ステップＳ２４２に進む。

ステップＳ２４２において、レシーバ５１の通信部６１は、ステップＳ２４１で相互認証したサービスプロバイダ３－１から、公開鍵証明書を受信する。

ステップＳ２４３において、レシーバ５１の復号／暗号化モジュール７４は、ステップＳ２４１で受信したサービスプロバイダセキュアコンテナに含まれる署名を検証し、改竄がなかったか否かを検証する。ここで、改竄が発見された場合、処理は終了するが、この例の場合、改竄が発見されなかったものとし、ステップＳ２４４に進む。

ステップＳ２４４において、ＵＣＰおよびＰＴが選択され、かつ、その利用内容および価格内容が選択される。具体的には、レシーバ５１の記憶モジュール７３に記憶されている基準情報５１（図３２）に基づいて、利用条件を満たすＵＣＰと価格条件を満たすＰＴが選択される。この例の場合、レシーバ５１の基準情

報５１の「利用ポイント情報」には、図３３に示したように、コンテンツプロバイダ２－１のコンテンツ利用ポイントが２２２ポイントであるとされている。すなわち、この基準情報５１によれば、コンテンツＡに対応して設定されたＵＣＰＡ，Ｂのうち、「利用条件１０」の「ユーザ条件１０」が”２００ポイント以上”とされているＵＣＰＡ（図１２Ａ）が選択される。また、基準情報５１の「決済ユーザ情報」には、ユーザＦは男性とされているので、ＰＴＡ－１（図２０Ａ）の「価格条件１０」に設定された条件を満たす。その結果、ＵＣＰＡに対応して作成されたＰＴＡ－１，ＰＴＡ－２のうち、ＰＴＡ－１が選択される。

その後、このようにして選択されたＵＣＰＡおよびＰＴＡ－１の内容が、表示制御部６７を介して、図示せぬ表示部に表示される。そこで、ユーザＦは、その表示を参照して（例えば、利用したい利用形式と、その価格を比較検討して）、ＵＣＰＡの所定の「利用内容」を選択するための操作を、図示せず操作部に対して行う。これにより、入力制御部６８を介して、選択されたＵＣＰＡの利用内容のＩＤおよびＰＴＡ－１のＩＤがＳＡＭ６２に出力される。なお、この例の場合、ＵＣＰＡの利用内容１１（ＰＴＡ－１の価格内容１１）が選択されたものとする。

ステップＳ２４５において、レシーバ５１のＳＡＭ６２の課金処理モジュール７２は、ステップＳ２４４で選択された、ＵＣＰＡの「利用内容１１」とＰＴＡ－１に基づいて、ＵＣＳＡ（図２８）および課金情報Ａ（図３０）を作成する。すなわち、この場合、コンテンツＡは、料金が２０００円で買い取り再生される。

ステップＳ２４６において、サービスプロバイダセキュアコンテナ（図２４）に含まれる、コンテンツＡ（コンテンツ鍵ＫｃｏＡで暗号化されている）、ＵＣＰＡ、ＰＴＡ－１，Ａ－２、およびコンテンツプロバイダ２の署名が取り出され、ＨＤＤ５２に出力され、記憶される。ステップＳ２４７において、復号／暗号化ユニット７４の復号ユニット９１は、サービスプロバイダセキュアコンテナに含まれるコンテンツ鍵ＫｃｏＡ（配送用鍵Ｋｄで暗号化されている）を、記憶モジ

ュール７３に記憶されている配送用鍵Ｋｄで復号する。

ステップＳ２４８において、復号／暗号化ユニット７４の暗号化ユニット９３は、ステップＳ２４７で復号されたコンテンツ鍵ＫｃｏＡを、記憶モジュール７３に記憶されている保存用鍵Ｋｓａｖｅで暗号化する。

ステップＳ２４９において、レシーバ５１のデータ検査モジュール７５は、ステップＳ２４８で保存用鍵Ｋｓａｖｅで暗号化されたコンテンツ鍵ＫｃｏＡ、およびステップＳ２４５で作成されたＵＣＳＡが対応して記憶される、外部記憶部６３の利用情報記憶部６３Ａ（図２９）の空き領域を有するブロックＢＰを検出する。この例の場合、利用情報記憶部６３Ａのブロック Ｂ Ｐ－１が検出される。なお、図２９の利用情報記憶部６３Ａにおいて、そのブロックＢＰ－１の利用情報用メモリ領域ＲＰ－３にコンテンツ鍵ＫｃｏＡおよびＵＣＳＡが記憶されているように示されているが、この例の場合、この時点において、それらは記憶されておらず、空いることを示す所定の初期情報が記憶されている。

ステップＳ２５０において、レシーバ５１のデータ検査モジュール７５は、ステップＳ２４９で検出したブロックＢＰ－１のデータ（利用情報用メモリ領域ＲＰ－１乃至ＲＰ－Ｎに記憶されている全てのデータ）にハッシュ関数を適用して、ハッシュ値を得る。次に、ステップＳ２５１において、データ検査モジュール７５は、ステップＳ２５０で得られたハッシュ値と、記憶モジュール７３に記憶されているブロックＢＰ－１に対応する検査値ＨＰ－１（図３１）とを比較し、一致するか否かを判定し、一致すると判定した場合、そのブロックＢＰ－１のデータは改竄されていないので、ステップＳ２５２に進む。

ステップＳ２５２において、レシーバ５１のＳＡＭ６２は、利用情報（ステップＳ２４８で、保存用鍵Ｋｓａｖｅで暗号化されたコンテンツ鍵ＫｃｏＡ、およびステップＳ２４５で作成されたＵＣＳＡ）を、外部記憶部６３のブロックＢＰ－１の利用情報用メモリ領域ＲＰ－３に記憶させる。

ステップＳ２５３において、レシーバ５１のデータ検査モジュール７５は、ステップＳ２５２で利用情報が記憶された利用情報用メモリ領域ＲＰ－３が属する

、利用情報記憶部６３ＡのブロックＢＰ－１に記憶されている全てのデータにハッシュ関数を適用してハッシュ値を算出し、ステップＳ２５４において、記憶モジュール７３に記憶されている検査値ＨＰ－１に上書きする。ステップＳ２５５において、課金処理モジュール７２は、ステップＳ２４５で作成した課金情報Ａを記憶モジュール７３に記憶させ、処理は終了する。

ステップＳ２５１において、算出されたハッシュ値と検査値ＨＰ－１とが一致しないと判定された場合、ブロックＢＰ－１のデータは改竄されているので、手続きは、ステップＳ２５６に進み、データ検査モジュール７５は、外部記憶部６３の利用情報記憶部６３Ａの全てのブロックＢＰを調べたか否かを判定し、外部記憶部６３の全てのブロックＢＰを調べていないと判定した場合、ステップＳ２５７に進み、利用情報記憶部６３Ａの、空きを有する他のブロックＢＰを検索し、ステップＳ２５０に戻り、それ以降の処理が実行される。

ステップＳ２５６において、外部記憶部６３の利用情報記憶部６３Ａの全てのブロックＢＰが調べられたと判定された場合、利用情報を記憶できるブロックＢＰ（利用情報用メモリ領域ＲＰ）は存在しないので、処理は終了する。

このように、サービスプロバイダセキュアコンテナが、レシーバ５１により受信されると、処理は終了し、図３９のステップＳ１５に進む。

（６－５）コンテンツの再生処理

ステップＳ１５において、供給されたコンテンツＡが、レシーバ５１において利用される。なお、この例の場合選択されたＵＣＰＡの利用内容１１によれば、コンテンツＡは、再生して利用される。そこで、ここでは、コンテンツＡの再生処理について説明する。この再生処理の詳細は、図４７のフローチャートに示されている。

ステップＳ２６１において、レシーバ５１のデータ検査モジュール７５は、図４６のステップＳ２５２で、コンテンツ鍵ＫｃｏＡ（保存用鍵Ｋｓａｖｅで暗号化されている）およびＵＣＳＡが記憶された利用情報用メモリ領域ＲＰ－３が属する、外部記憶部６３の利用情報記憶部６３ＡのブロックＢＰ－１のデータにハ

ッシュ関数を適用してハッシュ値を算出する。

ステップＳ２６２において、レシーバ５１のデータ検査モジュール７５は、ステップＳ２６１において算出したハッシュ値が、図４６のステップＳ２５３で算出し、ステップＳ２５４で記憶モジュール７３に記憶させたハッシュ値（検査値ＨＰ－１）と一致するか否かを判定し、一致すると判定した場合、ブロックＢＰ－１のデータは改竄されていないので、ステップＳ２６３に進む。

ステップＳ２６３において、ＵＣＳＡ（図２８）の「利用内容」の「パラメータ」に示されている情報に基づいて、コンテンツＡが利用可能か否かが判定される。例えば、「利用内容」の「形式」が、”期間制限再生”とされているＵＣＳにおいては、その「パラメータ」には、その開始期間（時刻）と終了期間（時刻）が記憶されているので、この場合、現在の時刻が、その範囲内にあるか否かが判定される。現在の時刻がその範囲内にあるとき、そのコンテンツの利用が可能であると判定され、範囲外にあるとき、利用不可と判定される。また、「利用内容」の「形式」が、所定の回数に限って再生（複製）する利用形式とされているＵＣＳにおいては、その「パラメータ」には、残された利用可能回数が記憶されている。この場合、「パラメータ」に記憶されている利用可能回数が０回でないとき、対応するコンテンツの利用が可能であると判定され、一方、利用可能回数が０回であるとき、利用不可と判定される。

なお、ＵＣＳＡの「利用内容」の「形式」は、”買い取り再生”とされているので、この場合、コンテンツＡは、買い取られ、制限なしに再生される。すなわち、ＵＣＳＡの「利用内容」の「パラメータ」には、コンテンツが利用可能であることを示す情報が設定されている。そのため、この例の場合では、ステップＳ２６３において、コンテンツＡが利用可能であると判定され、ステップＳ２６４に進む。

ステップＳ２６４において、レシーバ５１の課金モジュール７２は、ＵＣＳＡを更新する。ＵＣＳＡには、更新すべき情報は含まれていないが、例えば、「利用内容」の「形式」が所定の回数に限って再生する利用形式とされている場合、そ

の「パラメータ」に記憶されている、再生可能回数が１つだけデクリメントされる。

次に、ステップＳ２６５において、レシーバ５１のＳＡＭ６２は、ステップＳ２６４で更新されたＵＣＳＡ（この例の場合には、実際は、更新されていない）を、外部記憶部６３の利用情報記憶部６３Ａのブロック＃Ｐ－１の利用情報用メモリ領域ＲＰ－３に記憶させる。ステップＳ２６６において、データ検査モジュール７５は、ステップＳ２６５でＵＣＳＡが記憶された、外部記憶部６３の利用情報記憶部６３Ａのブロック＃Ｐ－１のデータにハッシュ関数を適用して、ハッシュ値を算出し、記憶モジュール７３に記憶されている検査値ＨＰ－１に上書きする。

ステップＳ２６７において、ＳＡＭ６２の相互認証モジュール７１と、伸張部６４の相互認証モジュール１０１は、相互認証し、ＳＡＭ６２および伸張部６４は、一時鍵Ｋｔｅｍｐを共有する。この認証処理は、図４１乃至図４３を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数Ｒ１、Ｒ２、Ｒ３、またはその組み合わせが、一時鍵Ｋｔｅｍｐとして用いられる。

ステップＳ２６８において、復号／暗号化モジュール７４の復号ユニット９１は、図４６のステップＳ２５２で外部記憶部６３の利用情報記憶部６３Ａのブロック＃Ｐ－１（利用情報用メモリ領域ＲＰ－３）に記憶されたコンテンツ鍵ＫｃｏＡ（保存用鍵Ｋｓａｖｅで暗号化されている）を、記憶モジュール７３に記憶された保存用鍵Ｋｓａｖｅで復号する。

次に、ステップＳ２６９において、復号／暗号化モジュール７４の暗号化ユニット９３は、復号されたコンテンツ鍵ＫｃｏＡを一時鍵Ｋｔｅｍｐで暗号化する。ステップＳ２７０において、ＳＡＭ６２は、一時鍵Ｋｔｅｍｐで暗号化されたコンテンツ鍵ＫｃｏＡを伸張部６４に送信する。

ステップＳ２７１において、伸張部６４の復号モジュール１０２は、コンテンツ鍵ＫｃｏＡを一時鍵Ｋｔｅｍｐで復号する。ステップＳ２７２において、伸張

部６４は、インタフェース６６を介して、ＨＤＤ５２に記録されたコンテンツＡ（コンテンツ鍵Ｋｃｏで暗号化されている）を受け取る。ステップＳ２７３において、伸張部６４の復号モジュール１０３は、コンテンツＡ（コンテンツ鍵Ｋｃｏで暗号化されている）をコンテンツ鍵ＫｃｏＡで復号する。

ステップＳ２７４において、伸張部６４の伸張モジュール１０４は、復号されたコンテンツＡをＡＴＲＡＣ２などの所定の方式で伸張する。ステップＳ２７５において、伸張部６４のウォータマーク付加モジュール１０５は、伸張されたコンテンツＡにレシーバ５１を特定する所定のウォータマーク（電子透かし）を挿入する。ステップＳ２７６において、コンテンツＡは、図示せぬスピーカなどに出力され、再生される。その後、処理は終了する。

ステップＳ２６２において、ステップＳ２６１において算出されたハッシュ値が、レシーバ５１の記憶モジュール７３に記憶された検査値ＨＰ－１と一致しないと判定された場合、またはステップＳ２６３において、コンテンツが利用不可と判定された場合、ステップＳ２７７において、ＳＡＭ６２は、表示制御部６７を介して、図示せぬ表示部にエラーメッセージを表示させる等の所定のエラー処理を実行し、処理は終了する。

このようにして、レシーバ５１において、コンテンツＡが再生（利用）されたとき、処理は終了し、図３９の処理も終了する。

なお、以上においては、コンテンツＡが、レシーバ５１において利用（購入）される場合を例として説明したが、レシーバ２０１も、レシーバ５１と同様に、コンテンツＡを利用することができる。ただし、レシーバ２０１の基準情報２０１の「利用ポイント情報」には、図３８に示したように、コンテンツプロバイダ２－１のコンテンツ利用ポイントが２３ポイントとされているので、ＵＣＰＡの「利用条件１０」の「ユーザ条件１０」の条件を満たさない。すなわち、この場合、ＵＣＰＡは選択されず、ＵＣＰＢが選択される。

次に、ＰＴが選択されるが、この場合、ＵＣＰＢが選択されているので、ＵＣＰＢに対応するＰＴＢ－１，Ｂ－２（図２２）のうちのいずれかが選択される。

ＰＴＢ－１の「価格条件３０」は、機器が従機器であることが条件とされ、またＰＴＢ－２の「価格条件４０」は、主機器であることが条件とされている。すなわち、主機器であるレシーバ２０１においては、ＰＴＢ－２が選択される。このように、機器およびそのユーザに設定された各種条件に基づいて、ＵＣＰ、ＵＣＰの利用内容、およびＰＴの選択範囲が決定される。

また、以上においては、ＵＣＰの「利用条件」またはＰＴの「価格条件」の「ユーザ条件」を、ユーザの性別や年齢に関する条件とする場合を例として説明したが、例えば、ユーザの住んでいる地域や誕生日などを条件とすることもできる。なお、この場合、図１５Ａのサービスコードの０３００ｈ乃至７ＦＦＦｈのコート値に、それらの条件の意味を設定する。

（６－６）決済処理

次に、レシーバ５１の課金が決済される場合の処理手順を、図４８のフローチャートを参照して説明する。なお、この処理は、計上された課金が所定の上限額（正式登録時の上限額または仮登録時の上限額）を超えた場合、または配送用鍵Ｋｄのバージョンが古くなり、例えば、図４６のステップＳ２４７で、コンテンツ鍵Ｋｃｏ（配送用鍵Ｋｄで暗号化されている）を復号することができなくなった場合（サービスプロバイダセキュアコンテナを受信することができなくなった場合）に開始される。

すなわち、ステップＳ３０１において、レシーバ５１とＥＭＤサービスセンタ１との相互認証が行われる。この相互認証は、図４１乃至図４３を参照して説明した場合と同様の処理であるので、その説明は省略する。

次に、ステップＳ３０２において、レシーバ５１のＳＡＭ６２は、ＥＭＤサービスセンタ１のユーザ管理部１８に証明書を送信する。ステップＳ３０３において、レシーバ５１のＳＡＭ６２は、記憶モジュール７３に記憶されている課金情報を、ステップＳ３０１でＥＭＤサービスセンタ１と共有した一時鍵Ｋｔｅｍｐで暗号化し、配送用鍵Ｋｄのバージョン、ＨＤＤ５２に記憶されているＵＣＰおよびＰＴ、並びに登録リストとともに、ＥＭＤサービスセンタ１に送信する。

ステップＳ３０４において、ＥＭＤサービスセンタ１のユーザ管理部１８は、ステップＳ３０３で、レシーバ５１から送信された情報を受信し、復号した後、ＥＭＤサービスセンタ１のユーザ管理部１８が、登録リストの「状態フラグ」に”停止”が設定されるべき不正行為がレシーバ５１において存在するか否かを確認する。

ステップＳ３０５において、ＥＭＤサービスセンタ１の課金請求部１９は、ステップＳ３０３で受信された課金情報を解析し、ユーザ（例えば、ユーザＦ）の支払い金額を算出する処理等を行う。次に、ステップＳ３０６において、ユーザ管理部１８は、ステップＳ３０５における処理により、決済が成功したか否かを確認する。

次に、ステップＳ３０７において、ＥＭＤサービスセンタ１のユーザ管理部１８は、ステップＳ３０４における確認結果、およびステップＳ３０６における確認結果に基づいて、レシーバ５１の登録条件を設定し、それに署名を付して、レシーバ５１の登録リストを作成する。

例えば、ステップＳ３０４で、不正行為が確認された場合、「状態フラグ」には”停止”が設定され、この場合、今後、全ての処理が停止される。すなわち、ＥＭＤシステムからのサービスを一切受けることができなくなる。また、ステップＳ３０６で、決済が成功しなかったことが確認された場合、「状態フラグ」には”制限あり”が設定され、この場合、すでに購入したコンテンツを再生する処理は可能とされるが、新たにコンテンツを購入する処理は実行できなくなる。

次に、ステップＳ３０８に進み、ＥＭＤサービスセンタ１のユーザ管理部１８は、最新バージョンの配送用鍵Ｋｄ（３ヶ月分の最新バージョンの配送用鍵Ｋｄ）を一時鍵Ｋｔｅｍｐで暗号化し、ステップＳ３０７で作成された登録リストとともにレシーバ５１に送信する。

ステップＳ３０９において、レシーバ５１のＳＡＭ６２は、ＥＭＤサービスセンタ１から送信された配送用鍵Ｋｄおよび登録リストを、通信部６１を介して受信し、復号した後、記憶モジュール７３に記憶させる。このとき、記憶モジュー

ル７３に記憶されていた課金情報は消去され、登録リストおよび配送用鍵Ｋｄが更新される。

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

また、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、ＣＤ－ＲＯＭ、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

上述の本発明の実施の形態のコンテンツプロバイダは、第１の情報に対応させて、利用条件および利用内容を含む第２の情報を記憶し、第１の情報に対応させて第２の情報を所定の機器に送信するようにしたので、利用条件に応じた第１の情報の配布を行うことが可能になる。

また、本発明の実施の形態のサービスプロバイダは、第１の情報の利用条件および利用内容を含む第２の情報に対応して、第１の情報の価格条件および価格内容を含む第３の情報を作成するようにし、第１の情報に対応させて第２の情報および第３の情報を、所定の機器に送信するようにしたので、条件に応じた価格で第１の情報を配布することか可能になる。

また、本発明の実施の形態のレシーバは、基準情報に対応して選択した利用条件に対応する利用内容に従って、コンテンツを利用し、基準情報に対応して選択した価格条件に対応する価格内容に従って、コンテンツの利用に対して、課金処理を実行するようにしたので、変化に富んだサービスを受けることができる。

産業上の利用の可能性

本発明は、音楽データ、動画像データ、静止画像データ、文書データ、プログラムデータなどの情報を暗号化し、配信する情報処理システムに適応できる。

請 求 の 範 囲

1．暗号化されている第１の情報を保持する保持手段と、

上記第１の情報の利用条件と上記利用条件に対応する利用内容を含む第２の情報を、上記第１の情報に対応させて記憶する記憶手段と、

上記保持手段により保持されている暗号化されている上記第１の情報と、上記記憶手段により記憶されている上記第２の情報を所定の機器に送信する送信手段と

を具備する情報処理装置。

2．暗号化されている第１の情報を保持する保持ステップと、

上記第１の情報の利用条件と上記利用条件に対応する利用内容を含む第２の情報を、上記第１の情報に対応させて記憶する記憶ステップと、

上記保持ステップで保持された暗号化されている上記第１の情報と、上記記憶ステップで記憶された上記第２の情報を所定の機器に送信する送信ステップと

を具備する情報処理方法。

3．暗号化されている第１の情報を保持する保持ステップと、

上記第１の情報の利用条件と上記利用条件に対応する利用内容を含む第２の情報を、上記第１の情報に対応させて記憶する記憶ステップと、

上記保持ステップで保持された暗号化されている上記第１の情報と、上記記憶ステップで記憶された上記第２の情報を所定の機器に送信する送信ステップと

を具備する処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供する提供媒体。

4．所定のプロバイダから送信されてくる、暗号化されている第１の情報、および上記第１の情報の利用条件と上記利用条件に対応する利用内容を含む第２の情報を受信する受信手段と、

上記受信手段により受信された上記第２の情報に対応して、上記第１の情報の価格条件と上記価格条件に対応する価格内容を含む第３の情報を作成する作成手段と、

上記受信手段により受信された暗号化されている上記第１の情報および上記第２の情報、並びに上記作成手段により作成された上記第３の情報を、所定の機器に送信する送信手段と

を具備する情報処理装置。

5．所定のプロバイダから送信されてくる、暗号化されている第１の情報、および上記第１の情報の利用条件と上記利用条件に対応する利用内容を含む第２の情報を受信する受信ステップと、

上記受信ステップで受信された上記第２の情報に対応して、上記第１の情報の価格条件と上記価格条件に対応する価格内容を含む第３の情報を作成する作成ステップと、

上記受信ステップで受信された暗号化されている上記第１の情報および上記第２の情報、並びに上記作成ステップで作成された上記第３の情報を、所定の機器に送信する送信ステップと

を具備する情報処理方法。

6．所定のプロバイダから送信されてくる、暗号化されている第１の情報、および上記第１の情報の利用条件と上記利用条件に対応する利用内容を含む第２の情報を受信する受信ステップと、

上記受信ステップで受信された上記第２の情報に対応して、上記第１の情報の価格条件と上記価格条件に対応する価格内容を含む第３の情報を作成する作成ス

テップと、

上記受信ステップで受信された暗号化されている上記第１の情報および上記第２の情報、並びに上記作成ステップで作成された上記第３の情報を、所定の機器に送信する送信ステップと

を具備する処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供する提供媒体。

７．所定の基準情報を記憶する記憶手段と、

所定のプロバイダから送信されてくる、暗号化されている第１の情報、上記第１の情報の利用条件と上記利用条件に対応する利用内容を含む第２の情報、および上記第１の情報の価格条件と上記価格条件に対応する価格内容を含む第３の情報を受信する受信手段と、

上記記憶手段に記憶されている上記基準情報に対応する、上記受信手段により受信された上記第２の情報の上記利用条件を選択する利用条件選択手段と、

上記記憶手段に記憶されている上記基準情報に対応する、上記受信手段により受信された上記第３の情報の上記価格条件を選択する価格条件選択手段と、

上記利用条件選択手段により選択された上利用条件に対応する上記利用内容に従って、暗号化されている上第１の情報を復号して、利用する利用手段と、

上記価格条件選択手段により選択された上記価格条件に対応する上記価格内容に従って、利用手段による利用に対する課金処理を実行する実行手段と

を具備する情報処理装置。

８．所定の基準情報を記憶する記憶ステップと、

所定のプロバイダから送信されてくる、暗号化されている第１の情報、上記記第１の情報の利用条件と上記記利用条件に対応する利用内容を含む第２の情報、および上記第１の情報の価格条件と上価格条件に対応する価格内容を含む第３の情報を受信する受信ステップと、

上記記憶ステップで記憶された上記基準情報に対応する、上記受信ステップで受信された上記第２の情報の上記利用条件を選択する利用条件選択ステップと、

上記記憶ステップで記憶された上記基準情報に対応する、上記受信ステップで受信された上記第３の情報の上記価格条件を選択する価格条件選択ステップと、

上記利用条件選択ステップで選択された上記利用条件に対応する上記利用内容に従って、暗号化されている上記第１の情報を復号して、利用する利用ステップと、

上記価格条件選択ステップで選択された上記価格条件に対応する上記価格内容に従って、上記利用ステップでの利用に対する課金処理を実行する実行ステップと

を具備する情報処理方法。

９．所定の基準情報を記憶する記憶ステップと、

所定のプロバイダから送信されてくる、暗号化されている第１の情報、上記第１の情報の利用条件と上記利用条件に対応する利用内容を含む第２の情報、および上記第１の情報の価格条件と上記価格条件に対応する価格内容を含む第３の情報を受信する受信ステップと、

上記記憶ステップで記憶された上記基準情報に対応する、上記受信ステップで受信された上記第２の情報の上記利用条件を選択する利用条件選択ステップと、

上記記憶ステップで記憶された上記基準情報に対応する、上記受信ステップで受信された上記第３の情報の上記価格条件を選択する価格条件選択ステップと、

上記利用条件選択ステップで選択された上記利用条件に対応する上記利用内容に従って、暗号化されている上記第１の情報を復号して、利用する利用ステップと、

上記価格条件選択ステップで選択された上記価格条件に対応する上記価格内容に従って、上記利用ステップでの利用に対する課金処理を実行する実行ステップと

を含むする処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供する提供媒体。

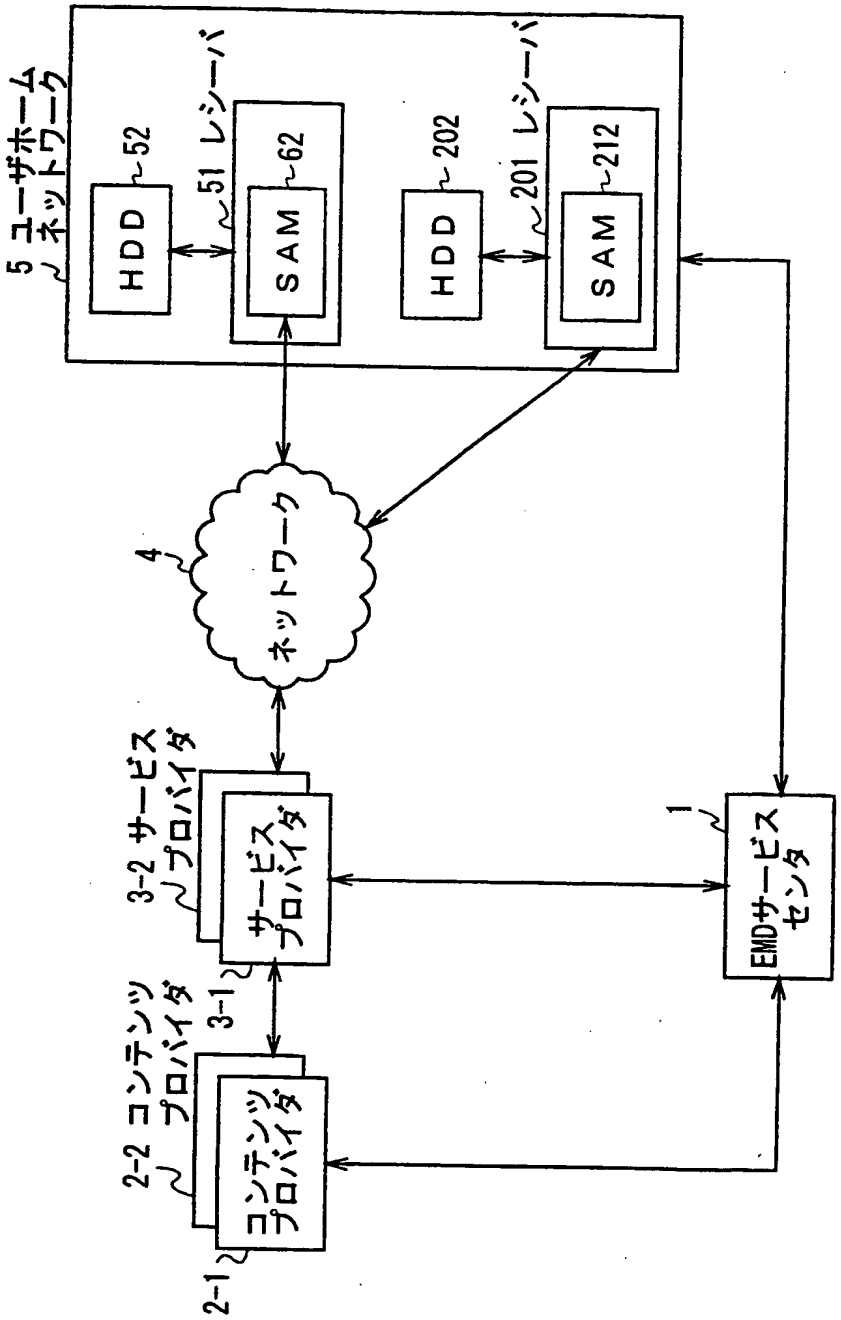

5 ユーザホーム ネットワーク
HDD
52
51 レシーバ
SAM
62
HDD
202
201 レシーバ
SAM
212
4
ネットワーク
3-2 サービス プロバイダ
サービス プロバイダ
3-1
2-2 コンテンツ プロバイダ
コンテンツ プロバイダ
2-1
1
EMDサービス センタ

図1

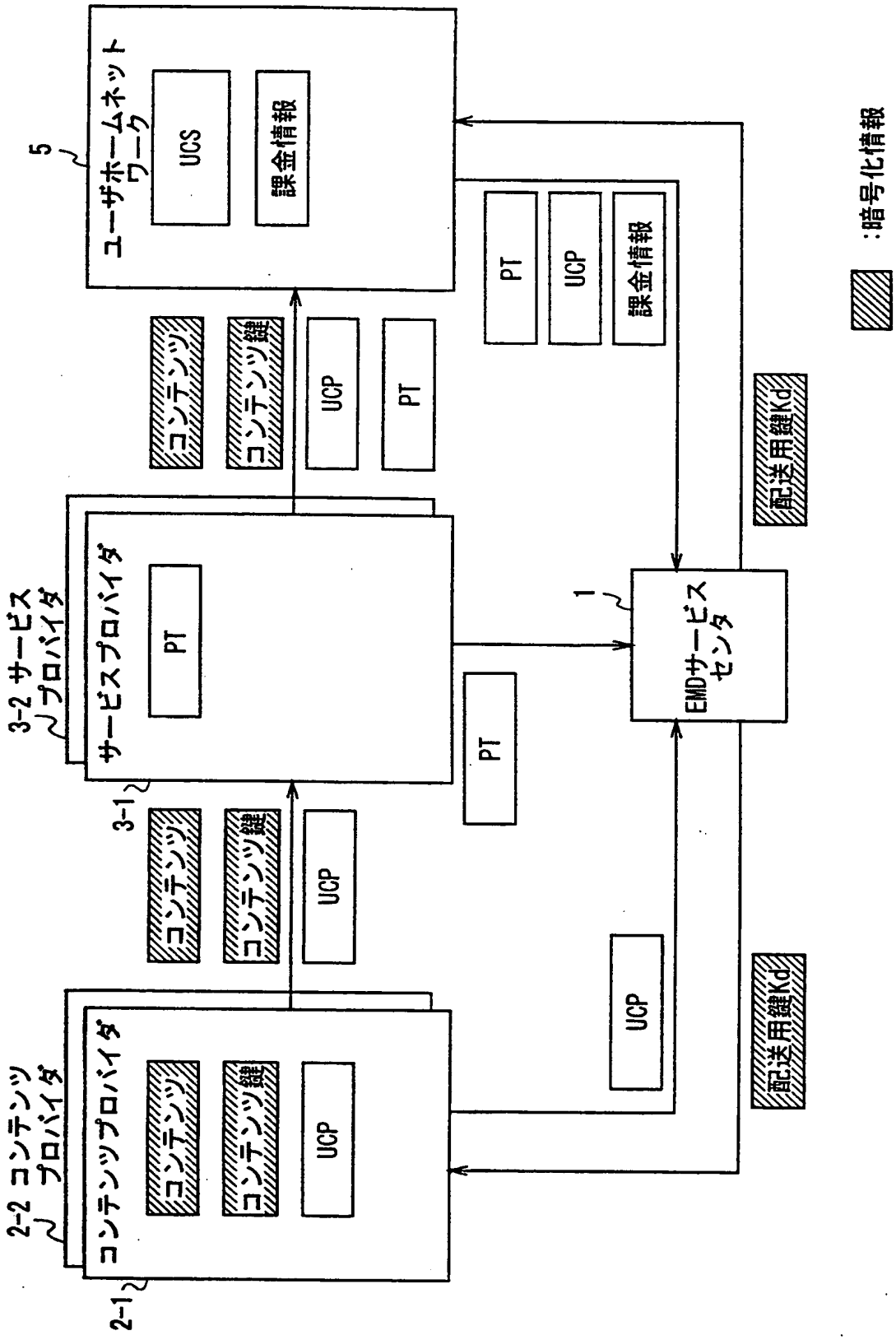
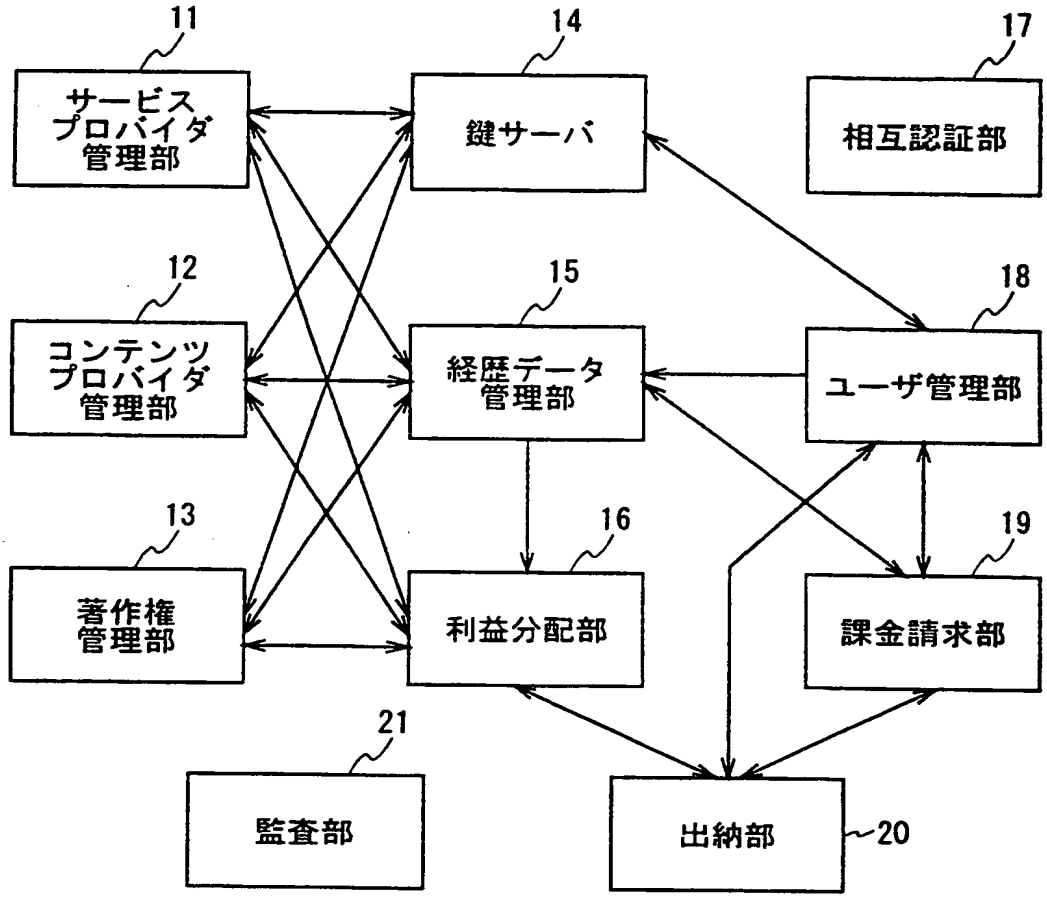

5
ユーザホームネットワーク
UCS
課金情報
PT
UCP
課金情報
コンテンツ
コンテンツ鍵
UCP
PT
3-2 サービスプロバイダ
サービスプロバイダ
PT
配送用鍵Kd
1
EMDサービスセンタ
PT
3-1
コンテンツ
コンテンツ鍵
UCP
UCP
2-2 コンテンツプロバイダ
コンテンツプロバイダ
コンテンツ
コンテンツ鍵
UCP
配送用鍵Kd
2-1
:暗号化情報

図2



EMDサービスセンタ 1

図３

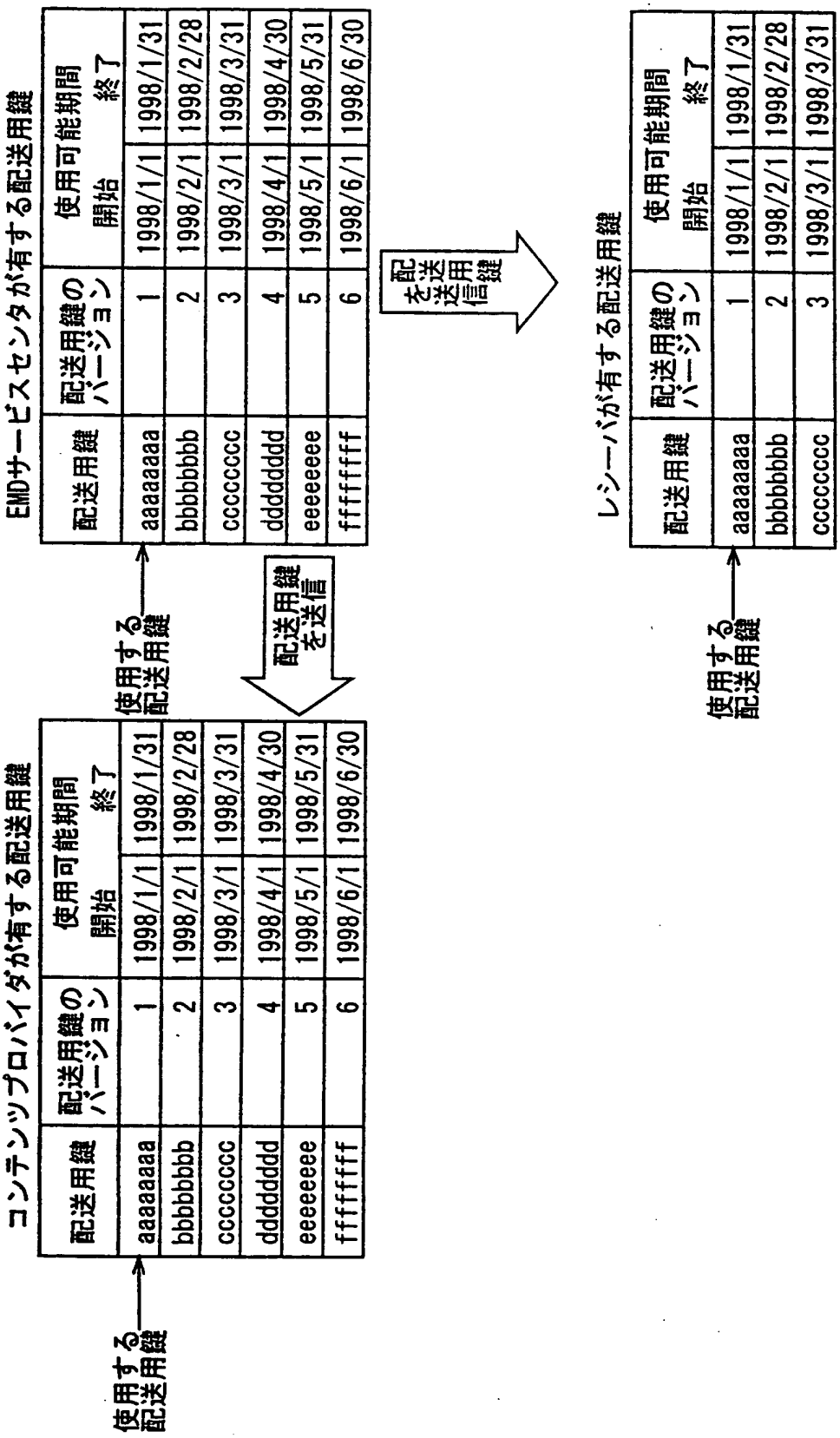

コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
使用する配送用鍵
使用する配送用鍵
配送用鍵を送信
EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
配送用鍵を送信
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
使用可能期間 終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
使用する配送用鍵

図4

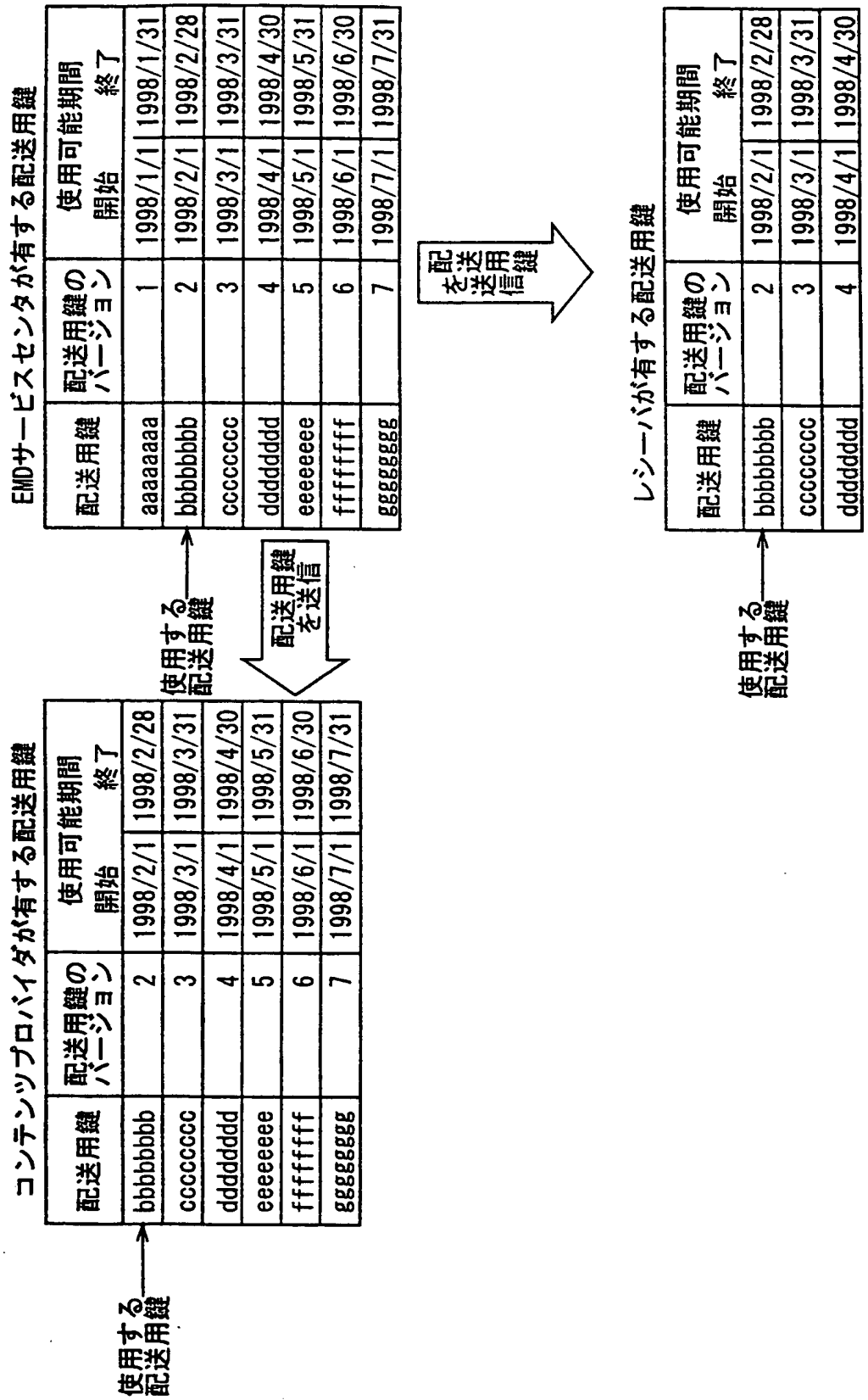

コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
終了
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
使用する配送用鍵
使用する配送用鍵
配送用鍵を送信
EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
終了
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
配を送送信鍵
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間 開始
終了
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
使用する配送用鍵

図5

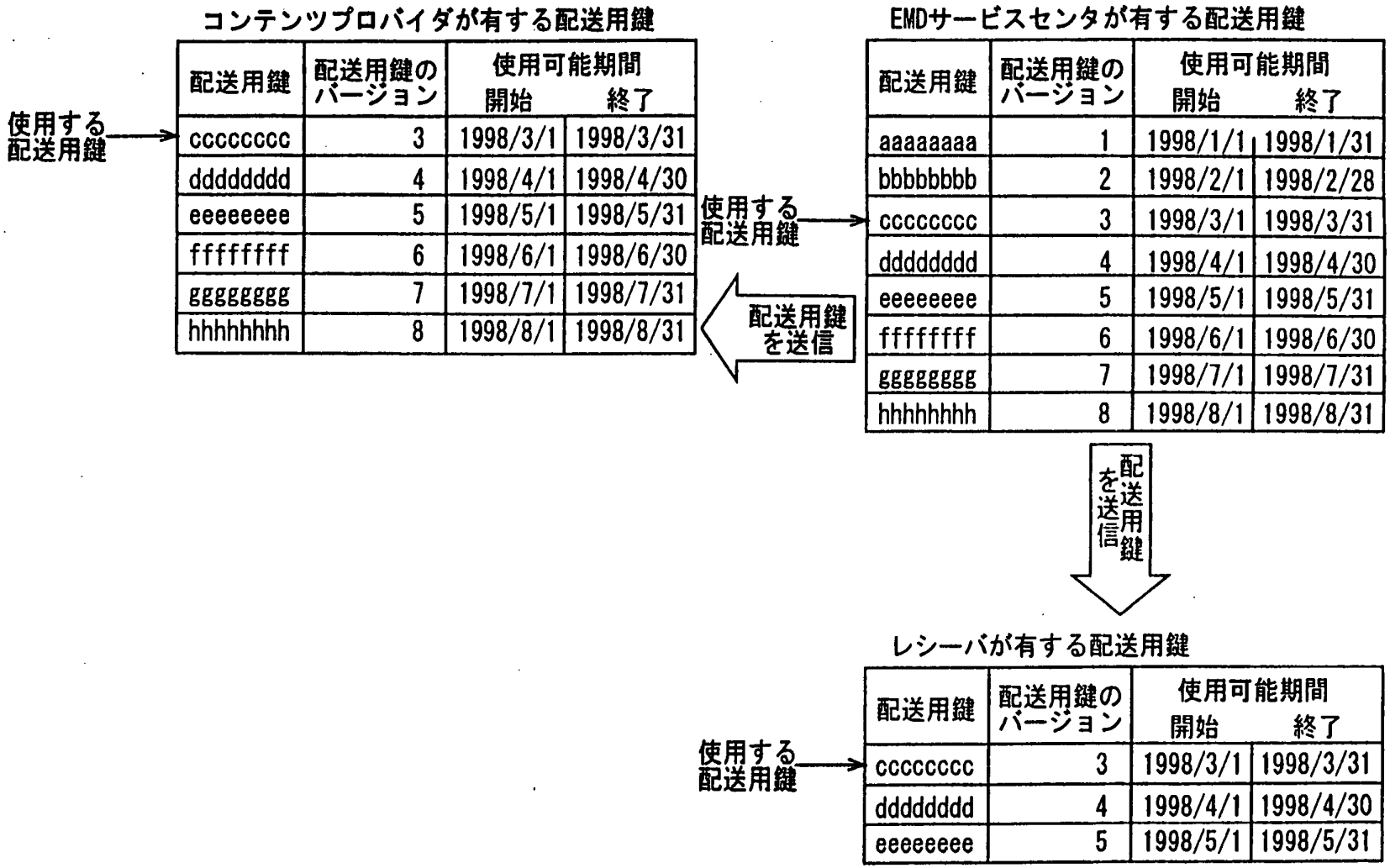

コンテンツプロバイダが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間
開始
終了
使用する配送用鍵
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
配送用鍵を送信
EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間
開始
終了
使用する配送用鍵
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
配送用鍵を送信
レシーバが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間
開始
終了
使用する配送用鍵
cccccccc 3 1998/3/1 1998/3/31
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31

図6

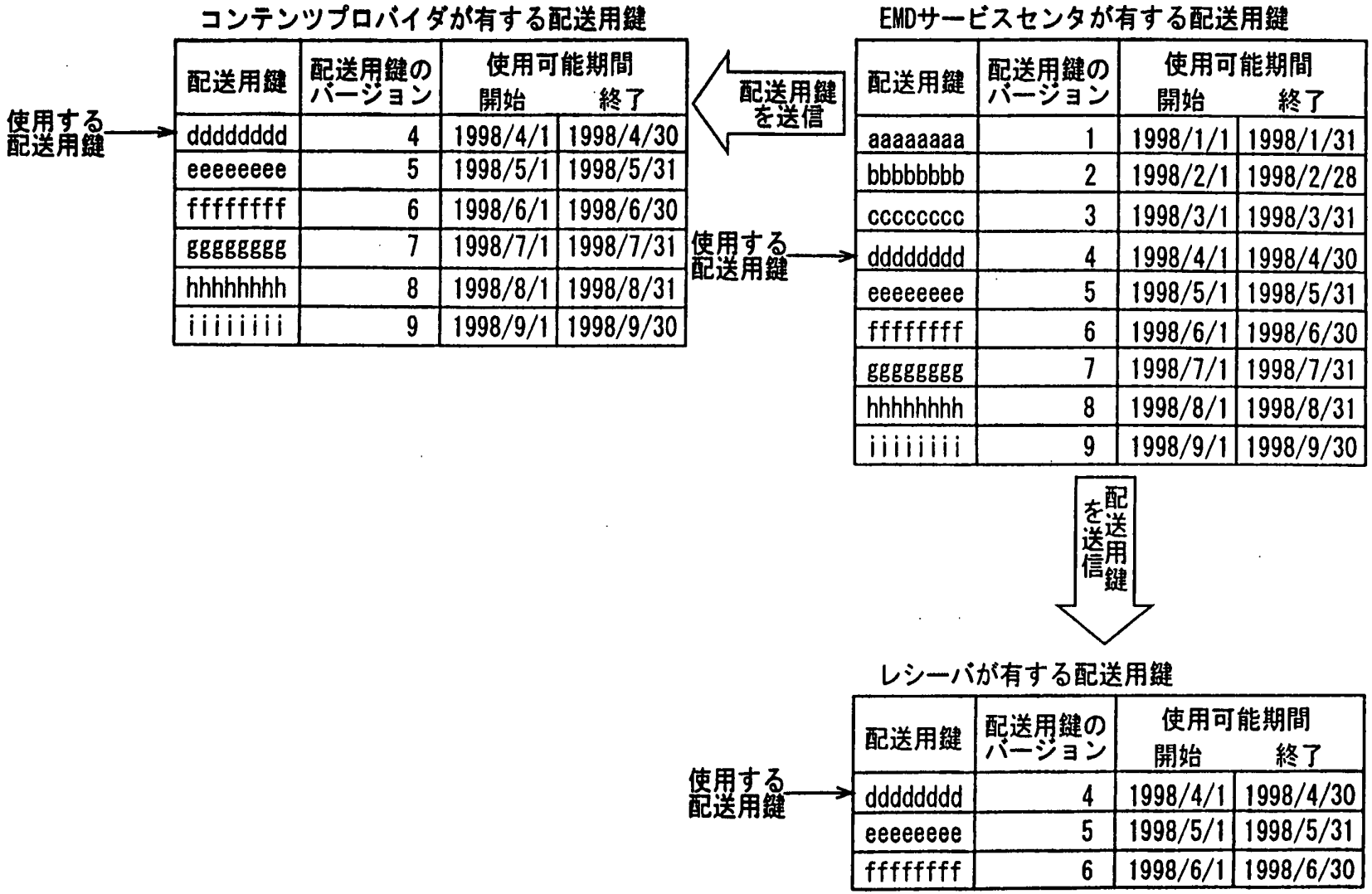

コンテンツプロバイダが有する配送用鍵
EMDサービスセンタが有する配送用鍵
配送用鍵
配送用鍵のバージョン
使用可能期間
開始
終了
使用する配送用鍵
配送用鍵を送信
dddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
iiiiiiii 9 1998/9/1 1998/9/30
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
レシーバが有する配送用鍵

図7

配送用鍵	配送用鍵のバージョン	使用可能期間 開始	終了
aaaaaaaaa	1	1998/1/1	1998/1/31

仮配送用鍵Kd

図８

SAMのID		SAM62のID	SAM212のID
機器番号		レシーバ51の機器番号(100番)	レシーバ201の機器番号(100番)
決済ID		ユーザFの決済ID	ユーザAの決済ID
決済ユーザ情報	氏名	ユーザFの氏名	ユーザAの氏名
	住所	ユーザFの住所	ユーザAの住所
	電話番号	ユーザFの電話番号	ユーザAの電話番号
	決済機関情報	ユーザFの決済情報	ユーザAの決済情報
	生年月日	ユーザFの生年月日	ユーザAの生年月日
	年齢	ユーザFの年齢	ユーザAの年齢
	性別	ユーザFの性別(男)	ユーザAの性別(女)
	ユーザのID	ユーザFのID	ユーザAのID
	パスワード	ユーザFのパスワード	ユーザAのパスワード
従属ユーザ情報	氏名		
	住所		
	電話番号		
	生年月日		
	性別		
	ユーザのID		
	パスワード		
利用ポイント情報		レシーバ51の利用ポイント情報	レシーバ201の利用ポイント情報

システム登録情報

図9

A

ユーザ	プロバイダ	利用ポイント
決済ユーザ	コンテンツプロバイダ2-1	222ポイント
	コンテンツプロバイダ2-2	123ポイント
	サービスプロバイダ3-1	345ポイント
	サービスプロバイダ3-2	0ポイント

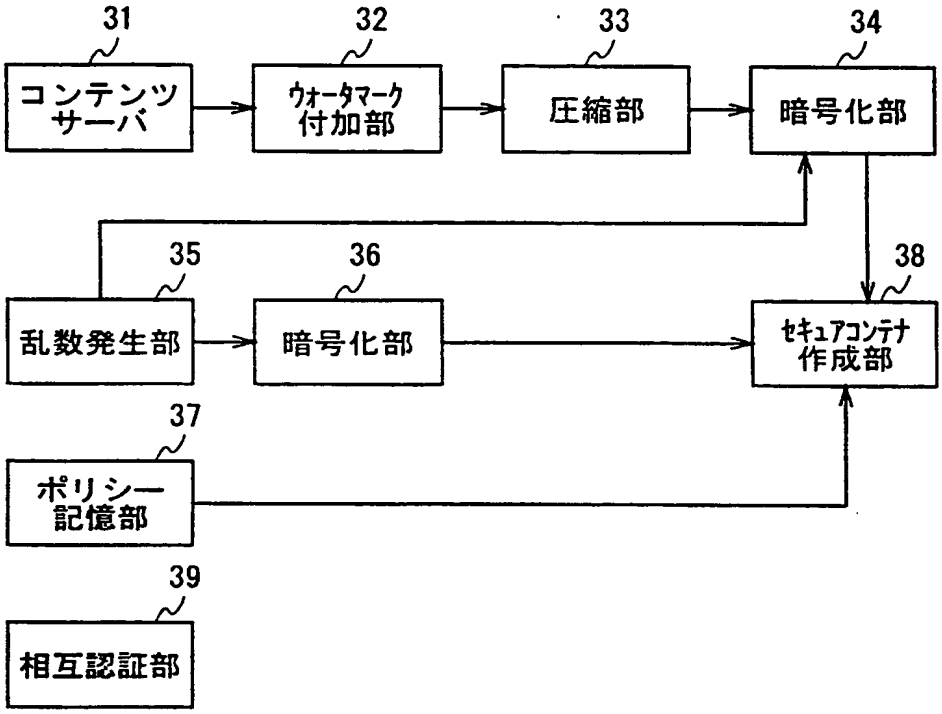
利用ポイント情報

B

ユーザ	プロバイダ	利用ポイント
決済ユーザ	コンテンツプロバイダ2-1	23ポイント
	コンテンツプロバイダ2-2	22ポイント
	サービスプロバイダ3-1	40ポイント
	サービスプロバイダ3-2	5ポイント

利用ポイント情報

図１０



コンテンツプロバイダ 2-1

図１１

A

コンテンツのID	コンテンツAのID	
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞのID	ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1のID	
UCPのID	UCPAのID	
UCPの有効期限	UCPAの有効期限	
利用条件 10	ﾕｰｻﾞ条件10	200ﾎﾟｲﾝﾄ以上
	機器条件10	条件なし
利用内容 11	ID 11	利用内容11のID
	形式11	買い取り再生
	ﾊﾟﾗﾒｰﾀ11	××××
	管理移動許可情報11	可
利用内容 12	ID 12	利用内容12のID
	形式12	第1世代複製
	ﾊﾟﾗﾒｰﾀ12	××××
	管理移動許可情報12	不可
利用内容 13	ID 13	利用内容13のID
	形式13	期間制限再生
	ﾊﾟﾗﾒｰﾀ13	××××
	管理移動許可情報13	不可
利用内容 14	ID 14	利用内容14のID
	形式14	Pay Per Copy 5
	ﾊﾟﾗﾒｰﾀ14	複製5回
	管理移動許可情報14	不可

UCPA

B

コンテンツのID		コンテンツAのID
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞのID		ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1のID
UCPのID		UCPBのID
UCPの有効期限		UCPBの有効期限
利用条件 20	ﾕｰｻﾞ条件20	200ﾎﾟｲﾝﾄより少ない
	機器条件20	条件なし
利用内容 21	ID 21	利用内容21のID
	形式21	Pay Per Play 4
	ﾊﾟﾗﾒｰﾀ21	再生4回
	管理移動許可情報21	不可
利用内容 22	ID 22	利用内容22のID
	形式22	Pay Per Copy 2
	ﾊﾟﾗﾒｰﾀ22	複製2回
	管理移動許可情報22	不可

UCPB

図１２

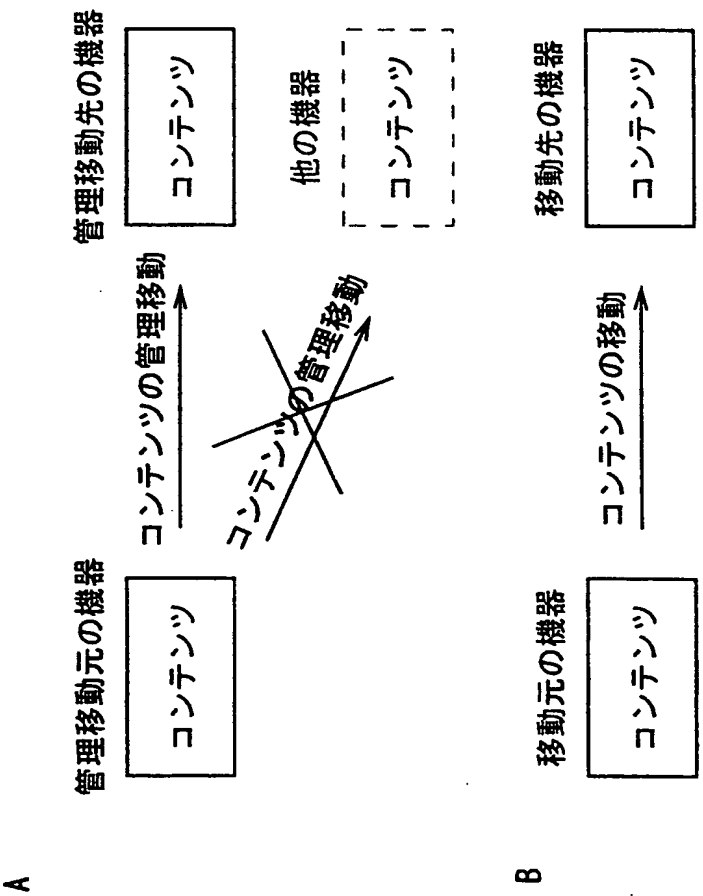

A
管理移動元の機器
コンテンツ
コンテンツの管理移動
管理移動先の機器
コンテンツ
他の機器
コンテンツ
コンテンツの管理移動
B
移動元の機器
コンテンツ
コンテンツの移動
移動先の機器
コンテンツ

図１３

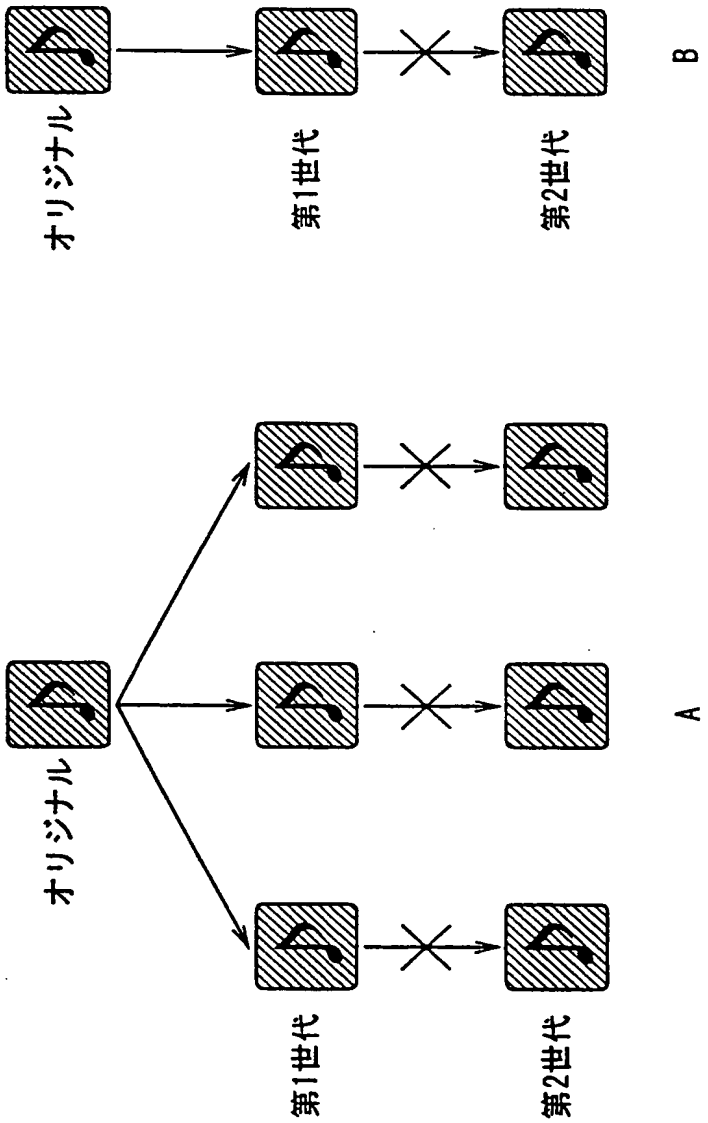


図１４

A

サービスコード	意味
0000h	条件なし
0001h乃至00FFh	機器に関し条件有り
0100h乃至01FFh	性別条件あり
0200h乃至02FFh	年令条件あり
0300h乃至7FFFh	その他の条件あり
8000h乃至FFFFh	利用ポイントに関し条件有り

B

コンディションコード	意味
00h	無条件
01h	＝
02h	≠
03h	＜(より小さい)
04h	＞(より大きい)
05h	≦(以下)
06h	≧(以上)
07h乃至FFh	空き

図１５

A

ユーザ条件 10	サービスコード	バリューコード	コンディションコード
	80×× h	0000C8h	06h
機器条件 10	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h

UCPAの利用条件 10

B

ユーザ条件 20	サービスコード	バリューコード	コンディションコード
	80×× h	0000C8h	03h
機器条件 20	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h

UCPBの利用条件 20

図１６

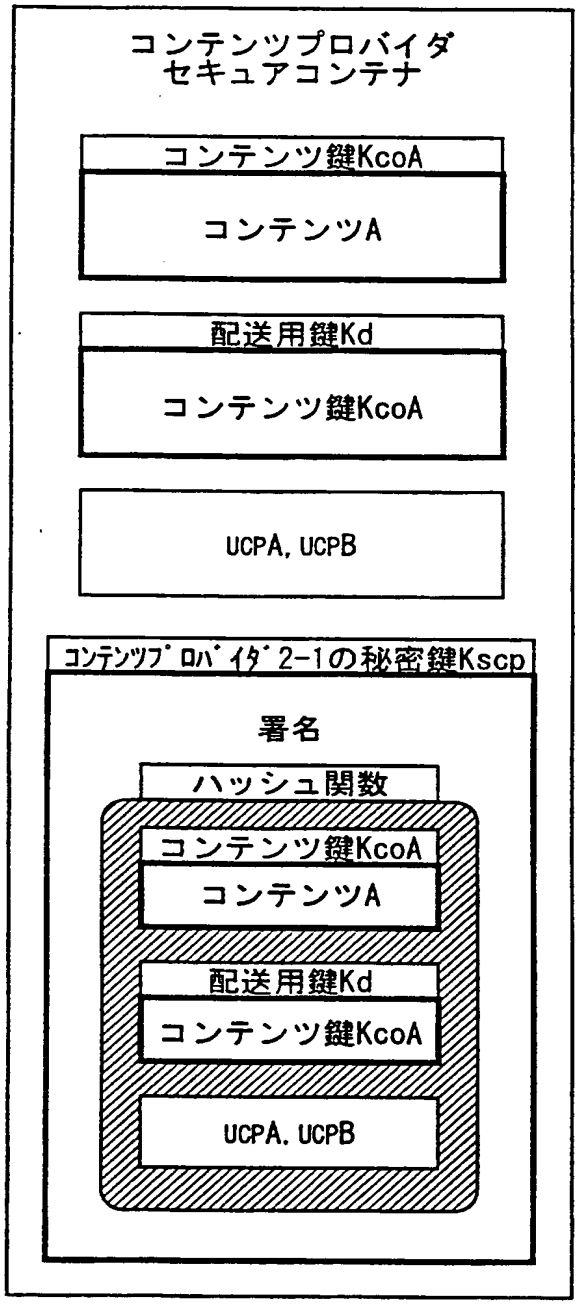

コンテンツプロバイダ
セキュアコンテナ
コンテンツ鍵KcoA
コンテンツA
配送用鍵Kd
コンテンツ鍵KcoA
UCPA, UCPB
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1の秘密鍵Kscp
署名
ハッシュ関数
コンテンツ鍵KcoA
コンテンツA
配送用鍵Kd
コンテンツ鍵KcoA
UCPA, UCPB

図１７

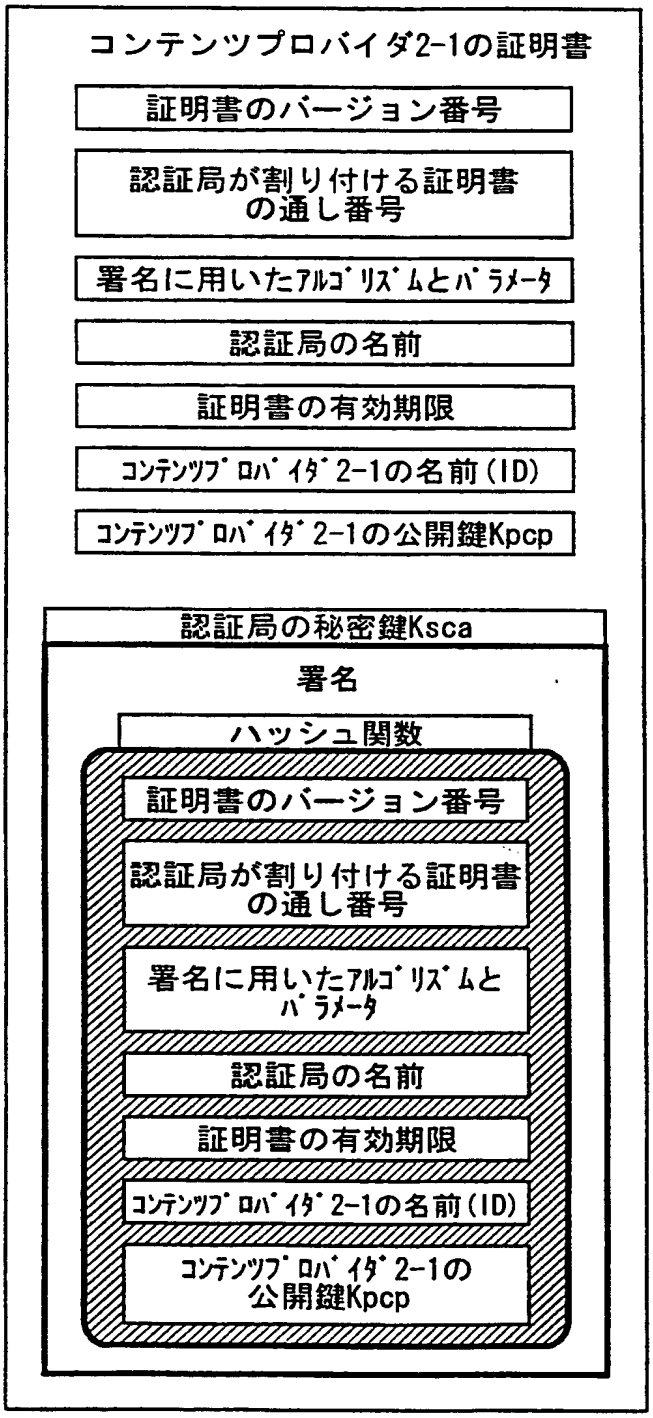
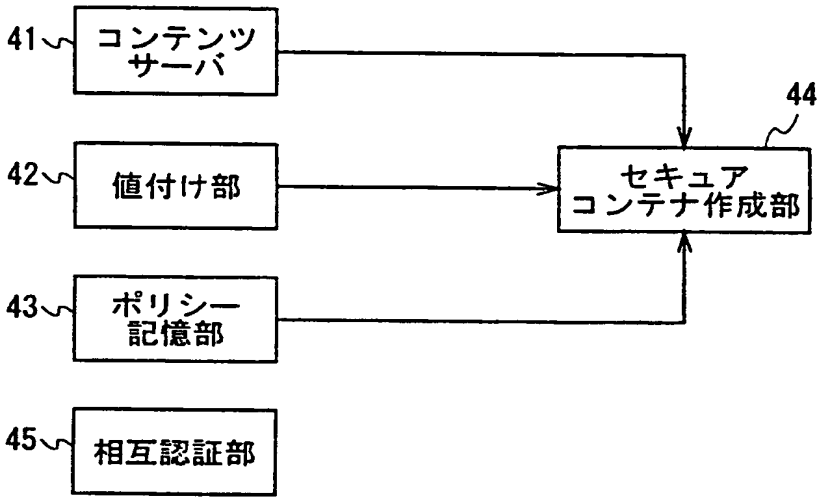

コンテンツプロバイダ2-1の証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたｱﾙｺﾞﾘｽﾞﾑとﾊﾟﾗﾒｰﾀ
認証局の名前
証明書の有効期限
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1の名前(ID)
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1の公開鍵Kpcp
認証局の秘密鍵Ksca
署名
ハッシュ関数
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたｱﾙｺﾞﾘｽﾞﾑとﾊﾟﾗﾒｰﾀ
認証局の名前
証明書の有効期限
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1の名前(ID)
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1の公開鍵Kpcp

図１８



サービスプロバイダ 3-1

図１９

A

コンテンツのID	コンテンツAのID	
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞのID	ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1のID	
UCPのID	UCPAのID	
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞのID	ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ3-1のID	
PTのID	PTA-1のID	
PTの有効期限	PTA-1の有効期限	
価格条件 10	ユーザ条件 10	男性
	機器条件 10	条件なし
価格内容 11	2000円	
価格内容 12	600円	
価格内容 13	100円	
価格内容 14	300円	

PTA-1

B

コンテンツのID	コンテンツAのID	
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞのID	ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1のID	
UCPのID	UCPAのID	
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞのID	ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ3-1のID	
PTのID	PTA-2のID	
PTの有効期限	PTA-2の有効期限	
価格条件 20	ユーザ条件 20	女性
	機器条件 20	条件なし
価格内容 21	1000円	
価格内容 22	300円	
価格内容 23	50円	
価格内容 24	150円	

PTA-2

図２０

A

ユーザ条件 10	サービスコード	バリューコード	コンディションコード
	01××h	000000h	01h
機器条件 10	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h

PTA-1の価格条件 10

B

ユーザ条件 20	サービスコード	バリューコード	コンディションコード
	01××h	000001h	01h
機器条件 20	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h

PTA-2の価格条件 20

図２１

コンテンツのID	コンテンツAのID	
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞのID	ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1のID	
UCPのID	UCPBのID	
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞのID	ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ3-1のID	
PTのID	PTB-1のID	
PTの有効期限	PTB-1の有効期限	
価格条件 30	ユーザ条件 30	条件なし
	機器条件 30	従機器
価格内容 31	100円	
価格内容 32	300円	

PTB-1

A

コンテンツのID	コンテンツAのID	
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞのID	ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1のID	
UCPのID	UCPBのID	
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞのID	ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ3-1のID	
PTのID	PTB-2のID	
PTの有効期限	PTB-2の有効期限	
価格条件 40	ユーザ条件 40	条件なし
	機器条件 40	主機器
価格内容 41	50円	
価格内容 42	150円	

PTB-2

B

図２２

A

ユーザ条件 30	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h
機器条件 30	サービスコード	バリューコード	コンディションコード
	00×× h	000064h	03h

PTB-1の価格条件 30

B

ユーザ条件 40	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h
機器条件 40	サービスコード	バリューコード	コンディションコード
	00×× h	000064h	06h

PTB-2の価格条件 40

図２３

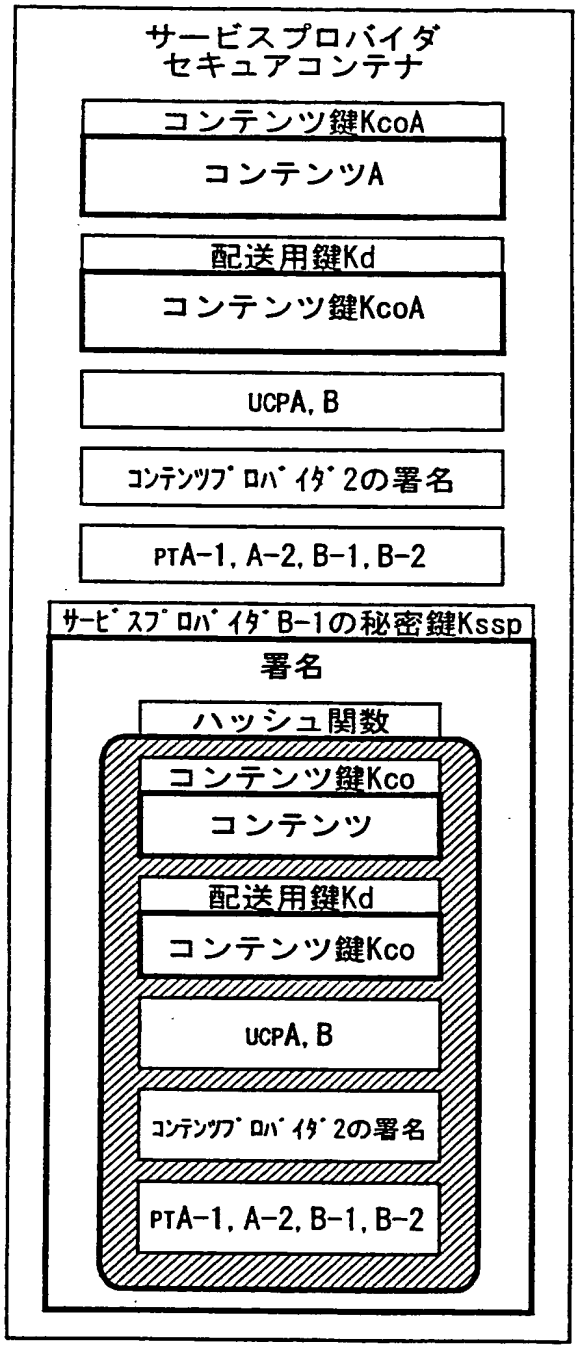

サービスプロバイダ
セキュアコンテナ
コンテンツ鍵KcoA
コンテンツA
配送用鍵Kd
コンテンツ鍵KcoA
UCPA, B
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2の署名
PTA-1, A-2, B-1, B-2
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞB-1の秘密鍵Kssp
署名
ハッシュ関数
コンテンツ鍵Kco
コンテンツ
配送用鍵Kd
コンテンツ鍵Kco
UCPA, B
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2の署名
PTA-1, A-2, B-1, B-2

図２４

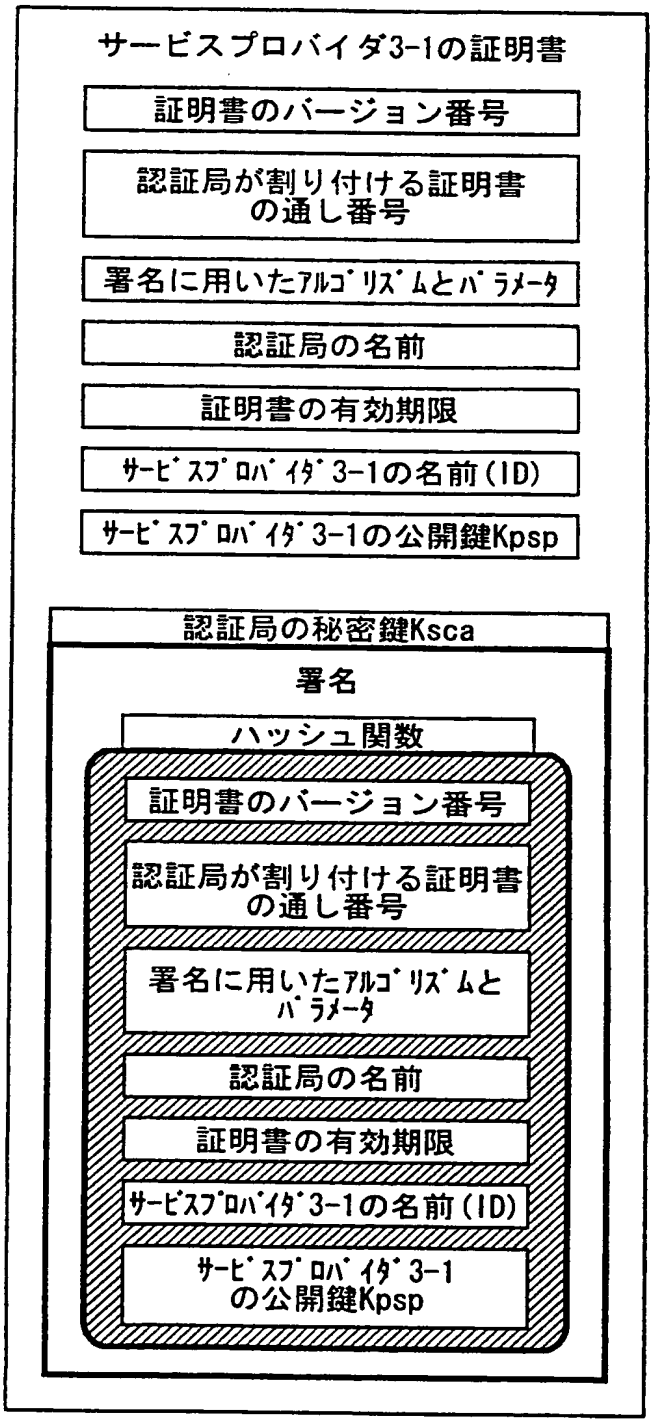

サービスプロバイダ3-1の証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたｱﾙｺﾞﾘｽﾞﾑとﾊﾟﾗﾒｰﾀ
認証局の名前
証明書の有効期限
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ3-1の名前(ID)
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ3-1の公開鍵Kpsp
認証局の秘密鍵Ksca
署名
ハッシュ関数
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたｱﾙｺﾞﾘｽﾞﾑとﾊﾟﾗﾒｰﾀ
認証局の名前
証明書の有効期限
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ3-1の名前(ID)
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ3-1の公開鍵Kpsp

図２５

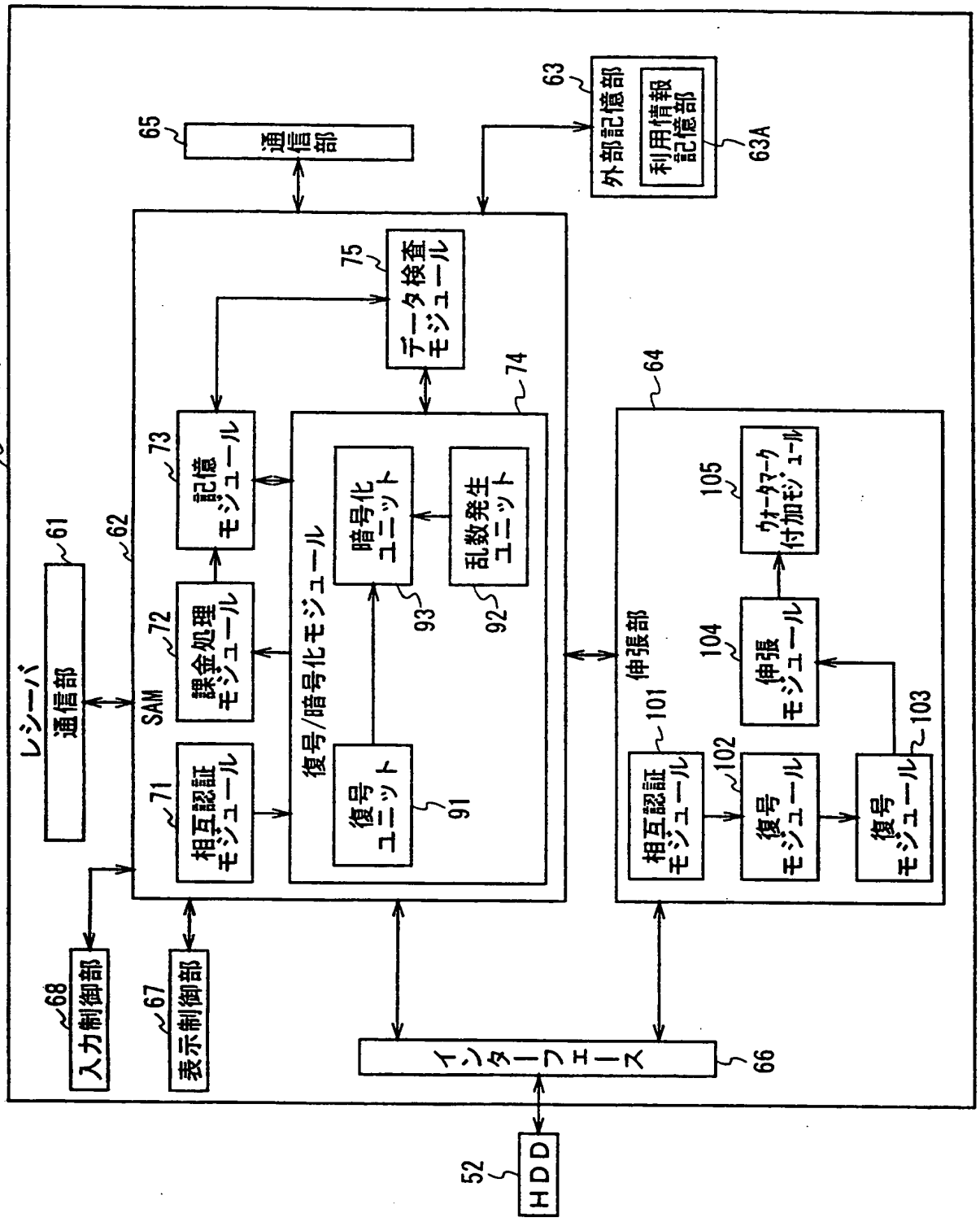

51 レシーバ
65 通信部
63 外部記憶部
利用情報記憶部
63A
75 データ検査モジュール
74
64
73 記憶モジュール
61
62
SAM
72 課金処理モジュール
暗号化ユニット
93
乱数発生ユニット
92
105 ウォータマーク付加モジュール
レシーバ
通信部
71 相互認証モジュール
復号/暗号化モジュール
復号ユニット
91
伸張部
104 伸張モジュール
101 相互認証モジュール
102 復号モジュール
103 復号モジュール
68 入力制御部
67 表示制御部
インターフェース
66
52 HDD

図26

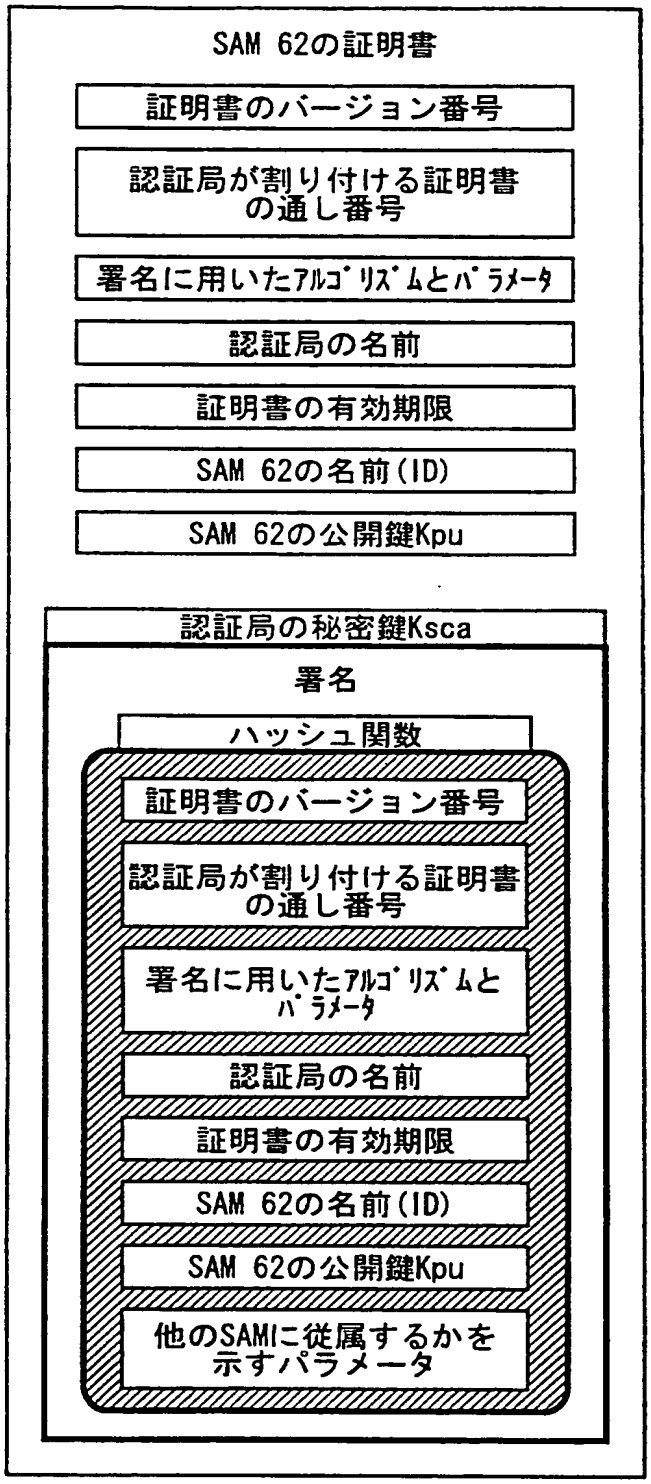

SAM 62の証明書
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたｱﾙｺﾞﾘｽﾞﾑとﾊﾟﾗﾒｰﾀ
認証局の名前
証明書の有効期限
SAM 62の名前(ID)
SAM 62の公開鍵Kpu
認証局の秘密鍵Ksca
署名
ハッシュ関数
証明書のバージョン番号
認証局が割り付ける証明書の通し番号
署名に用いたｱﾙｺﾞﾘｽﾞﾑとﾊﾟﾗﾒｰﾀ
認証局の名前
証明書の有効期限
SAM 62の名前(ID)
SAM 62の公開鍵Kpu
他のSAMに従属するかを示すパラメータ

図２７

コンテンツのID		コンテンツAのID
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞのID		ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1のID
UCPのID		UCPAのID
UCPの有効期限		UCPAの有効期限
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞのID		ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ3-1のID
PTのID		PTA-1のID
PTの有効期限		PTA-1の有効期限
UCSのID		UCSAのID
SAMのID		SAM62のID
ユーザのID		ユーザFのID
利用内容	ID	利用内容 11のID
	形式	買い取り再生
	パラメータ	××××
	管理移動状態情報	管理移動元:SAM62のID、 管理移動先:SAM62のID
利用履歴		××××

UCSA

図２８

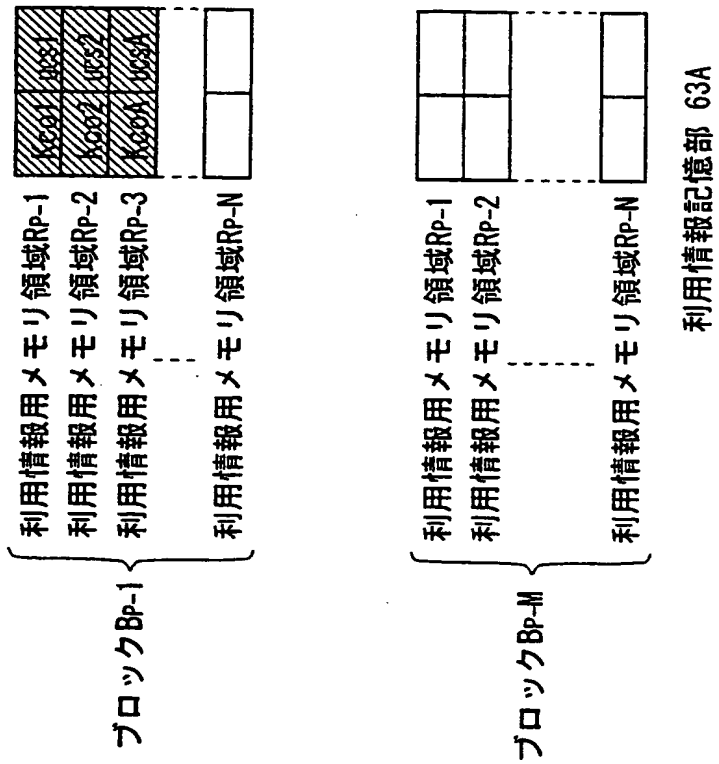

利用情報用メモリ領域Rp-1
利用情報用メモリ領域Rp-2
利用情報用メモリ領域Rp-3
利用情報用メモリ領域Rp-N
Kco1
Kco2
KcoA
US1
US2
USA
ブロックBp-1
利用情報用メモリ領域Rp-1
利用情報用メモリ領域Rp-2
利用情報用メモリ領域Rp-N
ブロックBp-M
利用情報記憶部 63A

図２９

コンテンツのID		コンテンツAのID
ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞのID		ｺﾝﾃﾝﾂﾌﾟﾛﾊﾞｲﾀﾞ2-1のID
UCPのID		UCPAのID
UCPの有効期限		UCPAの有効期限
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞのID		ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞ3-1のID
PTのID		PTA-1のID
PTの有効期限		PTA-1の有効期限
UCSのID		UCSAのID
SAMのID		SAM62のID
ユーザのID		ユーザFのID
利用内容	ID	利用内容11のID
	形式	買い取り再生
	パラメータ	×××
	管理移動状態情報	管理移動元:SAM62のID、 管理移動先:SAM62のID
課金履歴		×××

課金情報 A

図３０

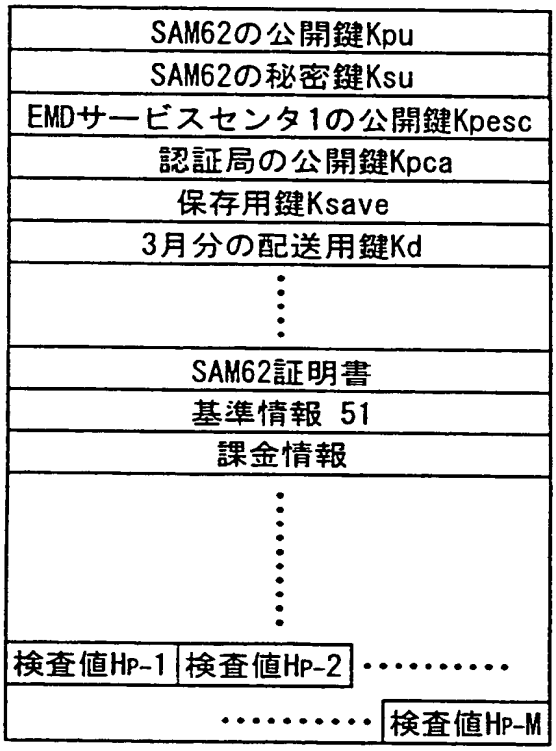

SAM62の公開鍵Kpu
SAM62の秘密鍵Ksu
EMDサービスセンタ1の公開鍵Kpesc
認証局の公開鍵Kpca
保存用鍵Ksave
3月分の配送用鍵Kd
SAM62証明書
基準情報 51
課金情報
検査値HP-1
検査値HP-2
検査値HP-M

図３１

SAMのID		SAM62のID
機器番号		レシーバ51の機器番号 (100番)
決済ID		ユーザFの決済ID
課金の上限額		正式登録時の 課金の上限額
決済ユーザ情報	氏名	ユーザFの氏名
	住所	ユーザFの住所
	電話番号	ユーザFの電話番号
	決済機関情報	ユーザFの決済機関情報
	生年月日	ユーザFの生年月日
	年齢	ユーザFの年齢(21才)
	性別	ユーザFの性別(男)
	ユーザのID	ユーザFのID
	パスワード	ユーザFのパスワード
従属ユーザ情報	氏名	
	住所	
	電話番号	
	生年月日	
	性別	
	ユーザのID	
	パスワード	
⋮		
利用ポイント情報		レシーバ51の利用 ポイント情報

基準情報 51

図３２

ユーザ	プロバイダ	利用ポイント
決済ユーザ	コンテンツプロバイダ 2-1	222ポイント
	コンテンツプロバイダ 2-2	123ポイント
	サービスプロバイダ 3-1	345ポイント
	サービスプロバイダ 3-2	0ポイント

基準情報51の利用ポイント情報

図３３

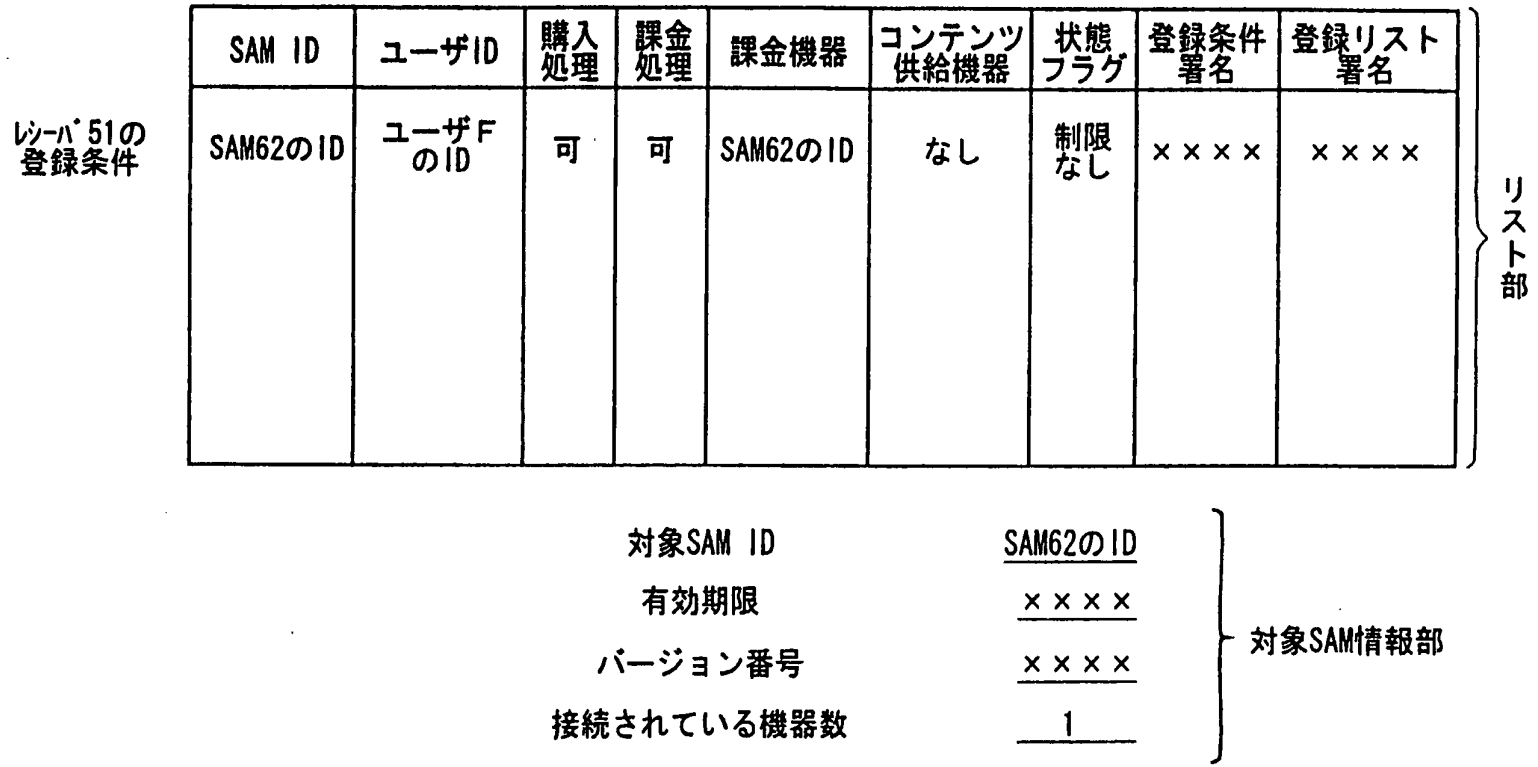

SAM ID
ユーザID
購入処理
課金処理
課金機器
コンテンツ供給機器
状態フラグ
登録条件署名
登録リスト署名
レシーバ51の登録条件
SAM62のID
ユーザFのID
可
可
SAM62のID
なし
制限なし
××××
××××
リスト部
対象SAM ID
SAM62のID
有効期限
××××
バージョン番号
××××
接続されている機器数
1
対象SAM情報部

図３４

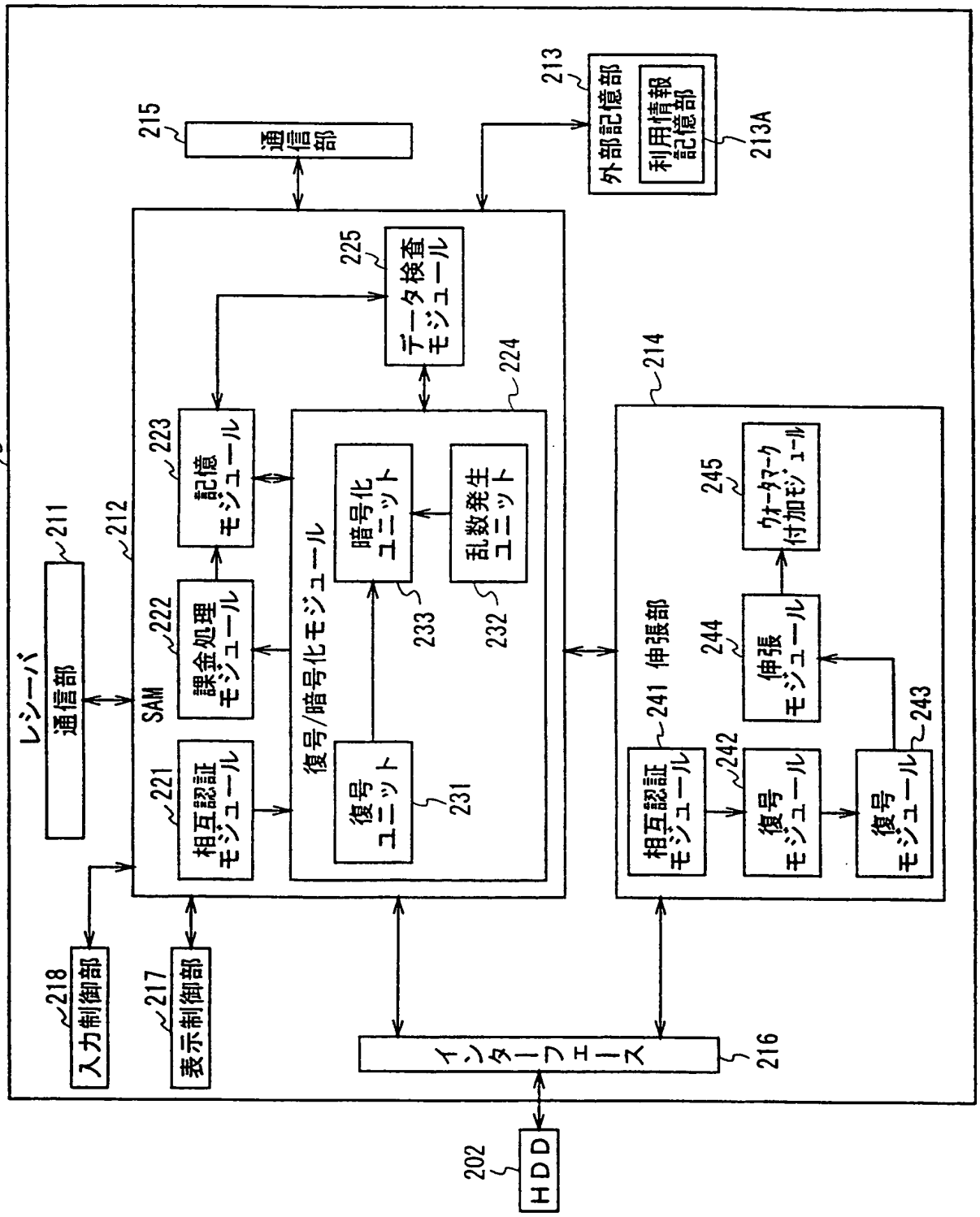

201 レシーバ
211
レシーバ
通信部
212
SAM
221
相互認証モジュール
222
課金処理モジュール
223
記憶モジュール
復号/暗号化モジュール
復号ユニット
231
暗号化ユニット
233
乱数発生ユニット
232
224
データ検査モジュール
225
215
通信部
213
外部記憶部
利用情報記憶部
213A
214
伸張部
241
相互認証モジュール
242
復号モジュール
243
伸張モジュール
244
ウォータマーク付加モジュール
245
218
入力制御部
217
表示制御部
インターフェース
216
202
HDD

図35

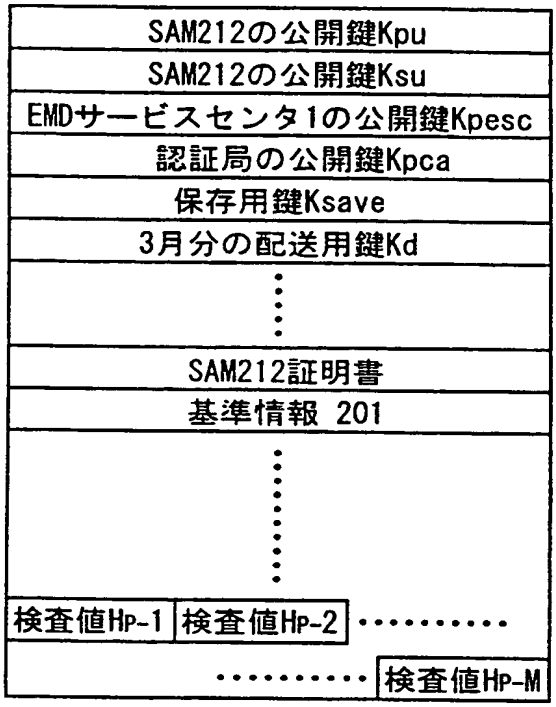

SAM212の公開鍵Kpu
SAM212の公開鍵Ksu
EMDサービスセンタ1の公開鍵Kpesc
認証局の公開鍵Kpca
保存用鍵Ksave
3月分の配送用鍵Kd
SAM212証明書
基準情報 201
検査値HP-1
検査値HP-2
検査値HP-M

図３６

SAMのID		SAM62のID
機器番号		ﾚｼｰﾊﾞ201の機器番号 (100番)
決済ID		ユーザAの決済ID
課金の上限額		正式登録時の 上限額
決済ユーザ情報	氏名	ユーザAの氏名
	住所	ユーザAの住所
	電話番号	ユーザAの電話番号
	決済機関情報	ユーザAの決済機関情報
	生年月日	ユーザAの生年月日
	年齢	ユーザAの年齢
	性別	ユーザAの性別
	ユーザのID	ユーザAのID
	パスワード	ユーザAのパスワード
従属ユーザ情報	氏名	
	住所	
	電話番号	
	生年月日	
	性別	
	ユーザのID	
	パスワード	
⋮		
利用ﾎﾟｲﾝﾄ情報		ﾚｼｰﾊﾞ201の利用 ﾎﾟｲﾝﾄ情報

基準情報 201

図３７

ユーザ	プロバイダ	利用ポイント
決済ユーザ	コンテンツプロバイダ2-1	23ポイント
	コンテンツプロバイダ2-2	22ポイント
	サービスプロバイダ3-1	40ポイント
	サービスプロバイダ3-2	5ポイント

基準情報201利用ポイント情報

図３８

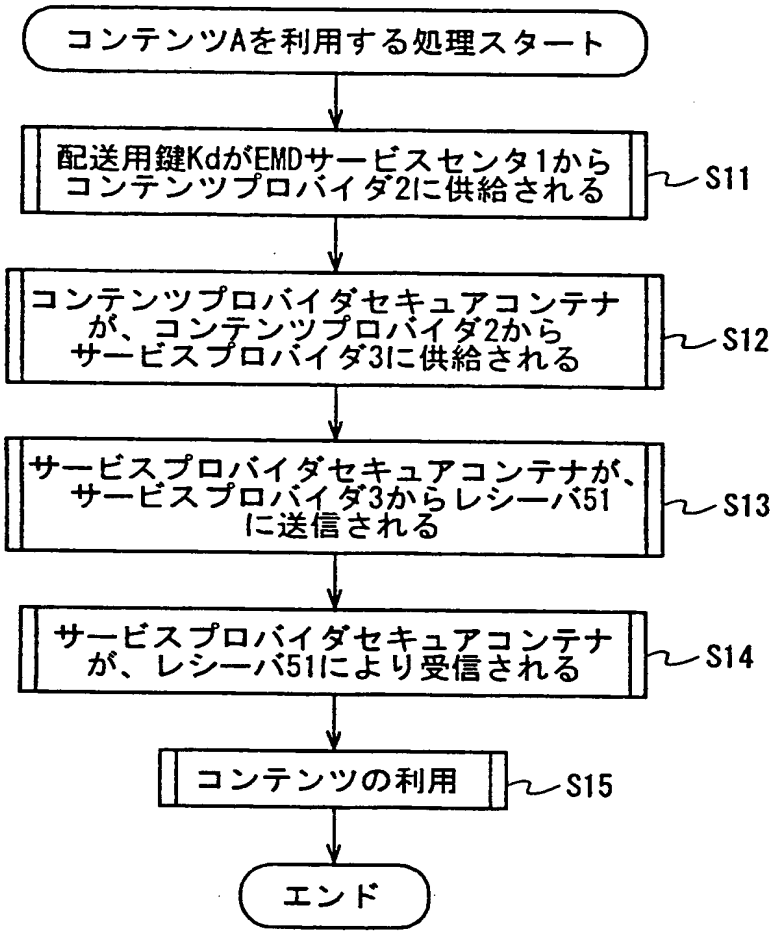

コンテンツAを利用する処理スタート
配送用鍵KdがEMDサービスセンタ1から
コンテンツプロバイダ2に供給される
S11
コンテンツプロバイダセキュアコンテナ
が、コンテンツプロバイダ2から
サービスプロバイダ3に供給される
S12
サービスプロバイダセキュアコンテナが、
サービスプロバイダ3からレシーバ51
に送信される
S13
サービスプロバイダセキュアコンテナ
が、レシーバ51により受信される
S14
コンテンツの利用
S15
エンド

図３９

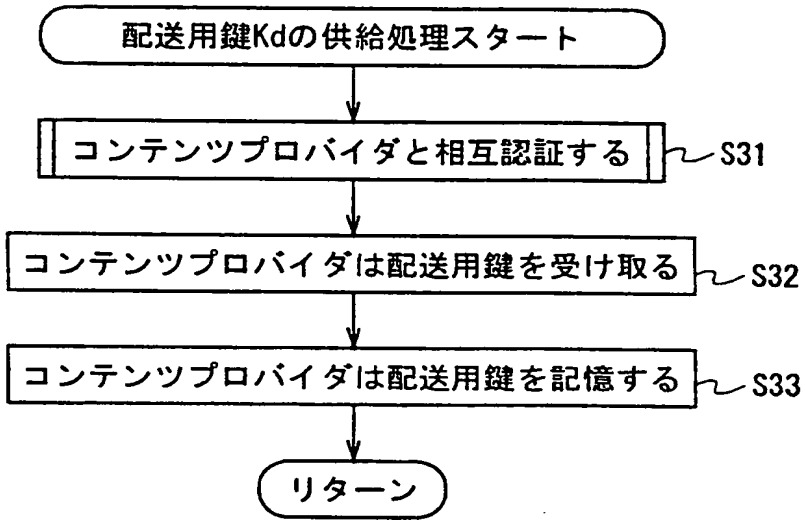

配送用鍵Kdの供給処理スタート
コンテンツプロバイダと相互認証する
S31
コンテンツプロバイダは配送用鍵を受け取る
S32
コンテンツプロバイダは配送用鍵を記憶する
S33
リターン

図４０

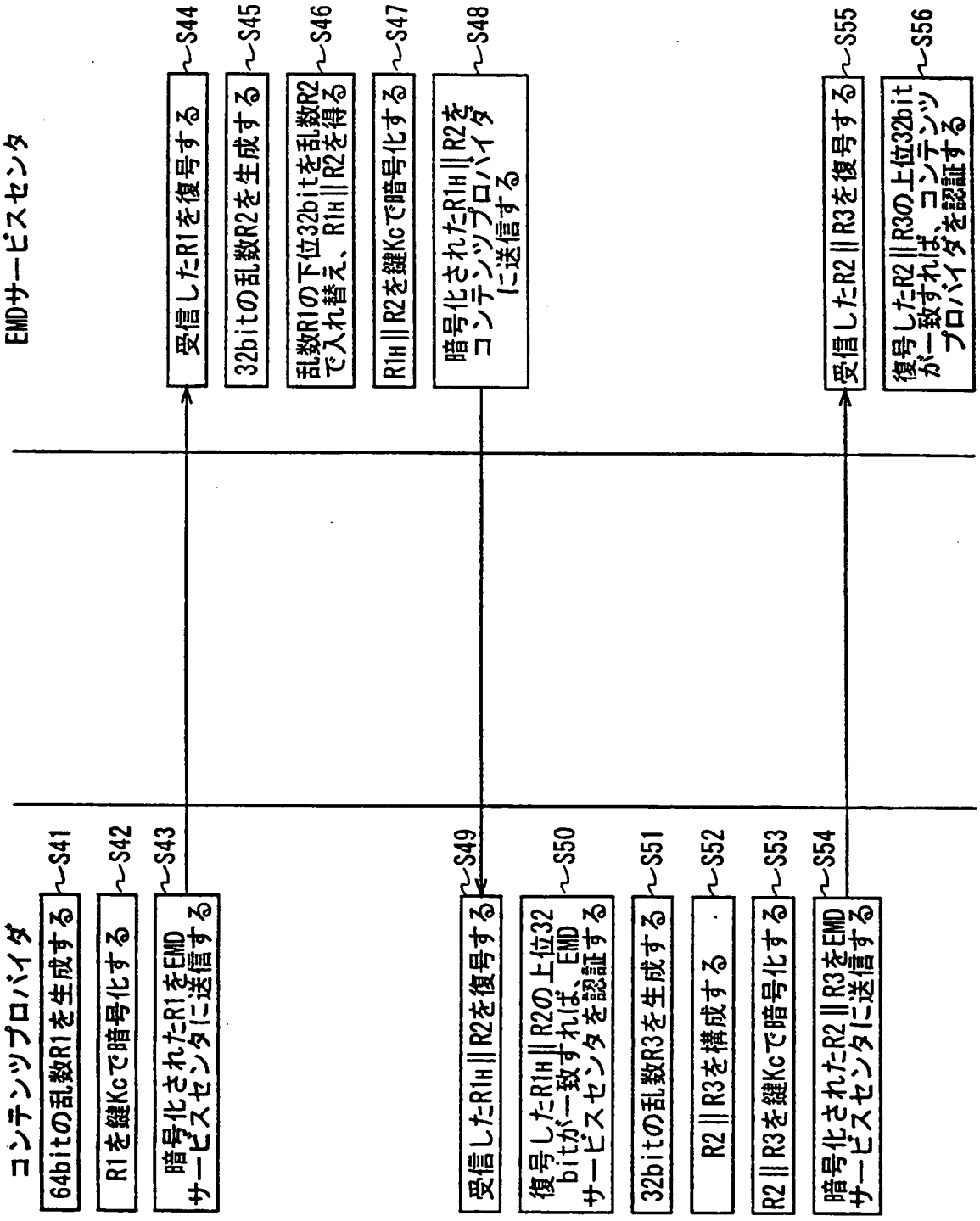

コンテンツプロバイダ
64bitの乱数R1を生成する
S41
R1を鍵Kcで暗号化する
S42
暗号化されたR1をEMD サービスセンタに送信する
S43
EMDサービスセンタ
受信したR1を復号する
S44
32bitの乱数R2を生成する
S45
乱数R1の下位32bitを乱数R2で入れ替え、R1H||R2を得る
S46
R1H||R2を鍵Kcで暗号化する
S47
暗号化されたR1H||R2をコンテンツプロバイダに送信する
S48
受信したR1H||R2を復号する
S49
復号したR1H||R2の上位32bitが一致すれば、EMD サービスセンタを認証する
S50
32bitの乱数R3を生成する
S51
R2||R3を構成する
S52
R2||R3を鍵Kcで暗号化する
S53
暗号化されたR2||R3をEMD サービスセンタに送信する
S54
受信したR2||R3を復号する
S55
復号したR2||R3の上位32bitが一致すれば、コンテンツプロバイダを認証する
S56

図41

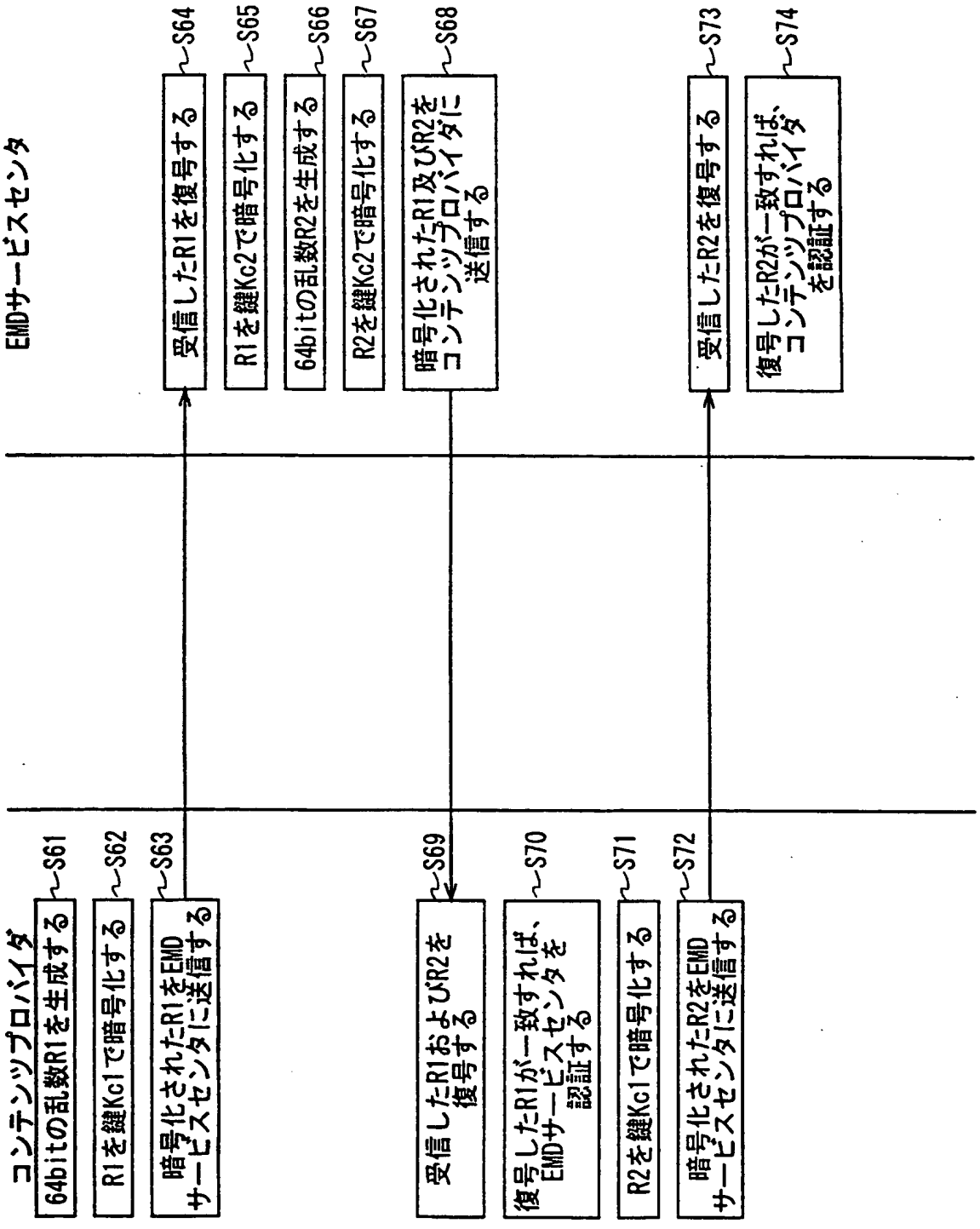

コンテンツプロバイダ
64bitの乱数R1を生成する
S61
R1を鍵Kc1で暗号化する
S62
暗号化されたR1をEMDサービスセンタに送信する
S63
受信したR1を復号する
S64
R1を鍵Kc2で暗号化する
S65
64bitの乱数R2を生成する
S66
R2を鍵Kc2で暗号化する
S67
暗号化されたR1及びR2をコンテンツプロバイダに送信する
S68
受信したR1およびR2を復号する
S69
復号したR1がEMDサービスセンタを認証する
S70
R2を鍵Kc1で暗号化する
S71
暗号化されたR2をEMDサービスセンタに送信する
S72
受信したR2を復号する
S73
復号したR2が一致すれば、コンテンツプロバイダを認証する
S74
EMDサービスセンタ

図42

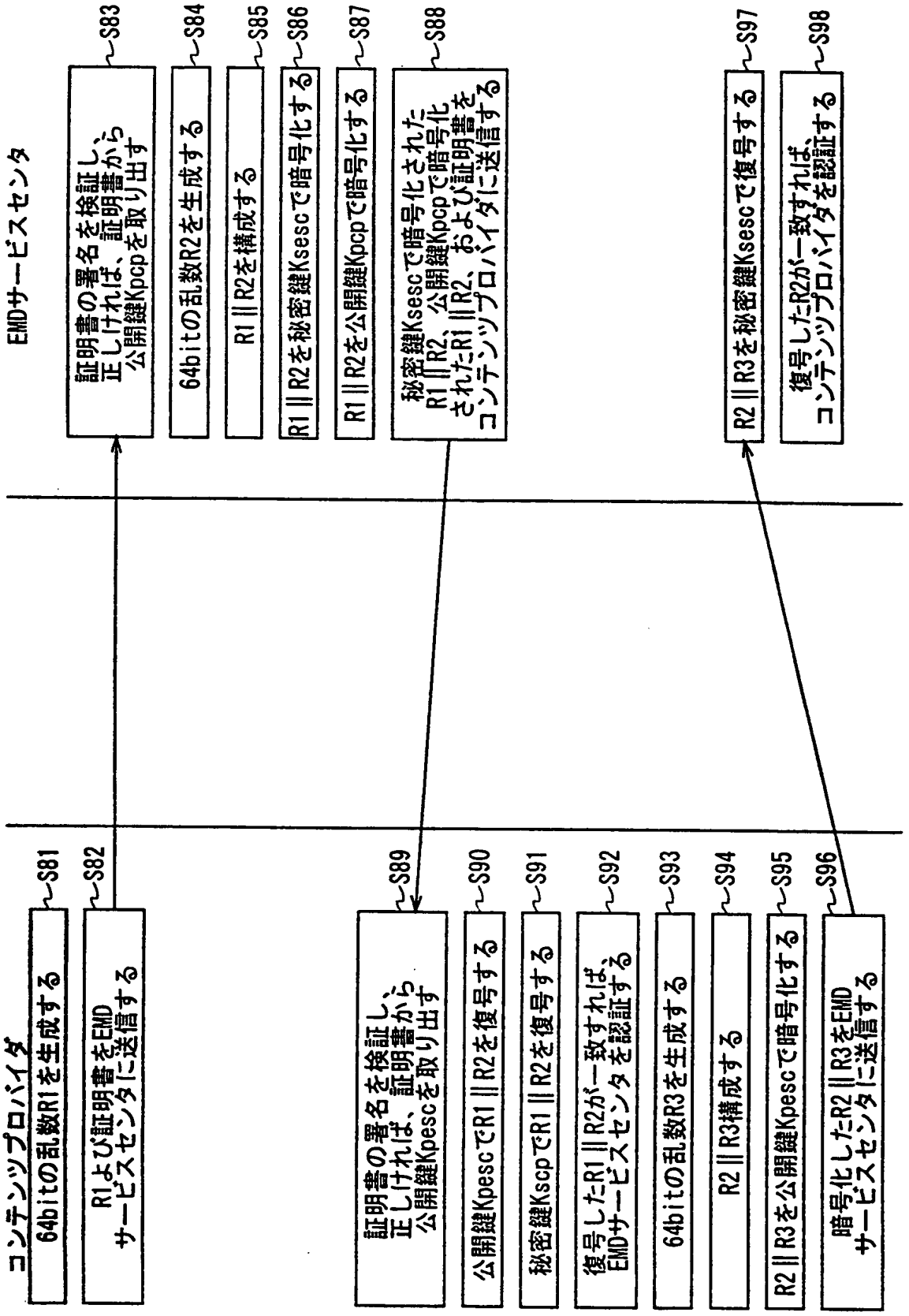

コンテンツプロバイダ
EMDサービスセンタ
64bitの乱数R1を生成する
S81
R1および証明書をEMDサービスセンタに送信する
S82
証明書の署名を検証し、正しければ、証明書から公開鍵Kpcpを取り出す
S83
64bitの乱数R2を生成する
S84
R1 || R2を構成する
S85
R1 || R2を秘密鍵Ksescで暗号化する
S86
R1 || R2を公開鍵Kpcpで暗号化する
S87
秘密鍵Ksescで暗号化されたR1 || R2、公開鍵Kpcpで暗号化されたR1 || R2、および証明書をコンテンツプロバイダに送信する
S88
証明書の署名を検証し、正しければ、証明書から公開鍵Kpescを取り出す
S89
公開鍵KpescでR1 || R2を復号する
S90
秘密鍵KscpでR1 || R2を復号する
S91
復号したR1 || R2がEMDサービスセンタを認証する
S92
64bitの乱数R3を生成する
S93
R2 || R3構成する
S94
R2 || R3を公開鍵Kpescで暗号化する
S95
暗号化したR2 || R3をEMDサービスセンタに送信する
S96
R2 || R3を秘密鍵Ksescで復号する
S97
復号したR2が一致すれば、コンテンツプロバイダを認証する
S98

図43

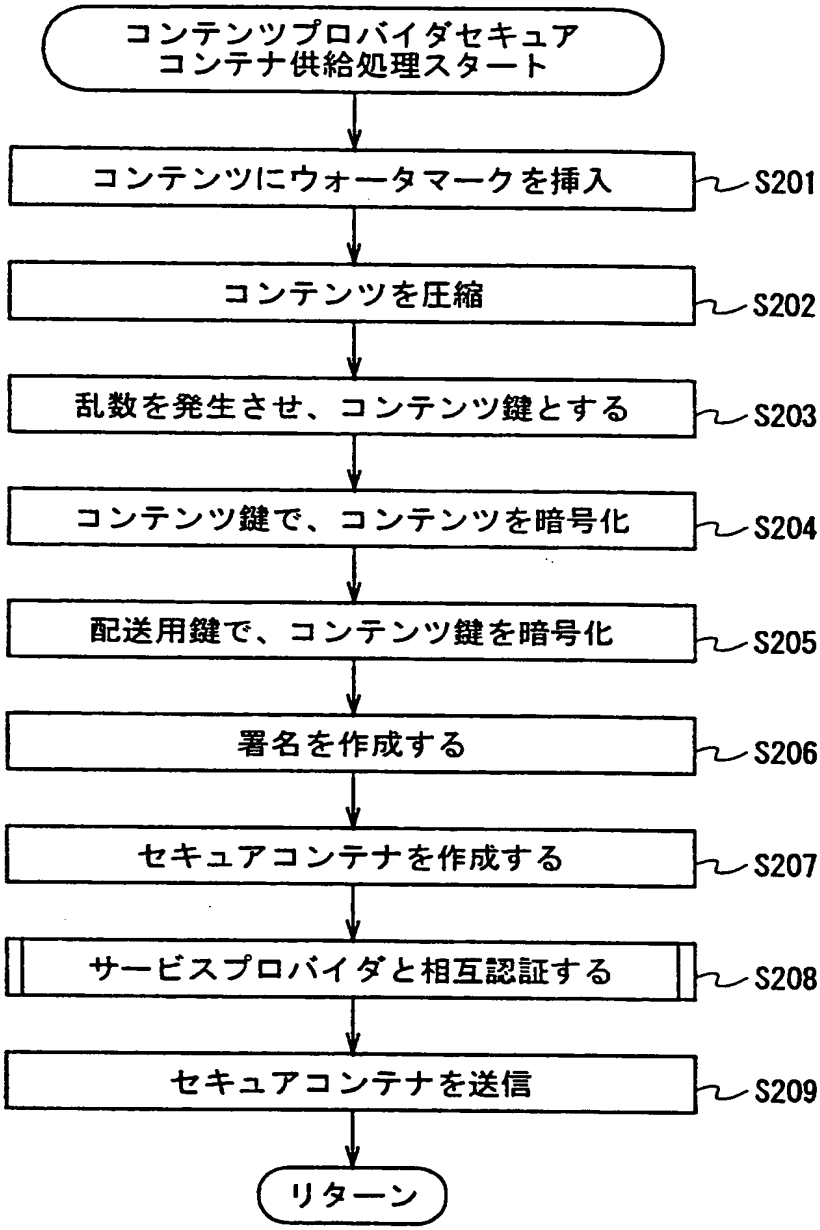

コンテンツプロバイダセキュア
コンテナ供給処理スタート
コンテンツにウォータマークを挿入
S201
コンテンツを圧縮
S202
乱数を発生させ、コンテンツ鍵とする
S203
コンテンツ鍵で、コンテンツを暗号化
S204
配送用鍵で、コンテンツ鍵を暗号化
S205
署名を作成する
S206
セキュアコンテナを作成する
S207
サービスプロバイダと相互認証する
S208
セキュアコンテナを送信
S209
リターン

図４４

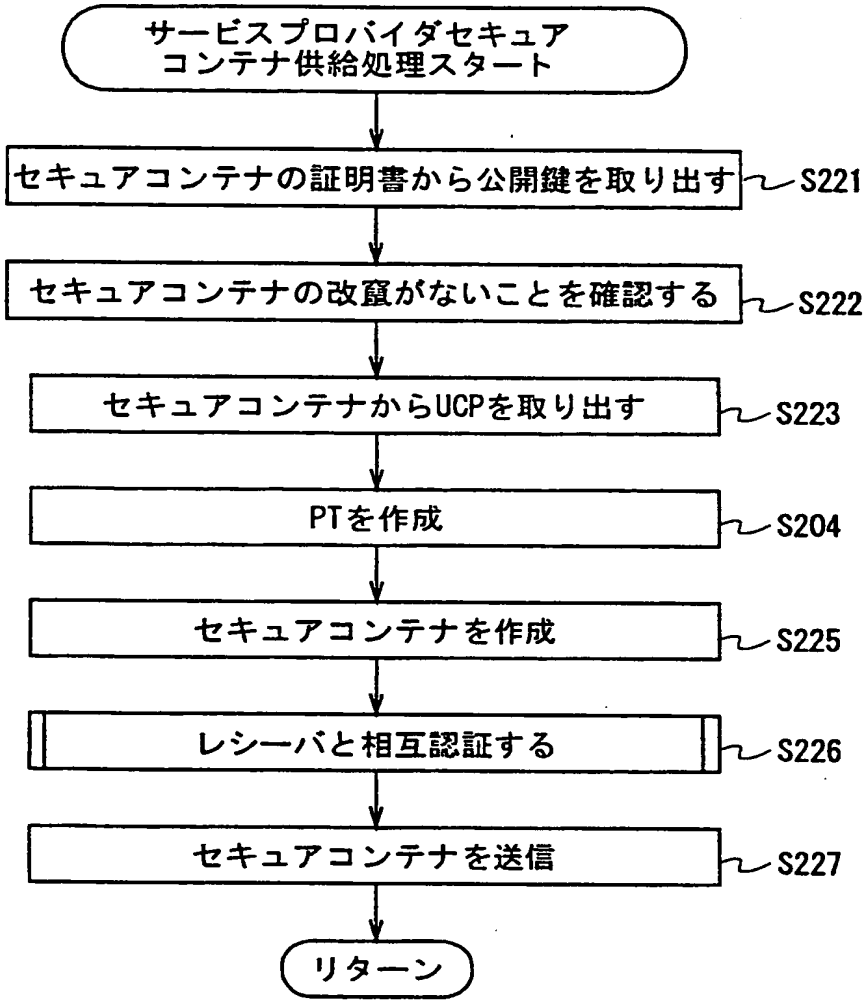

サービスプロバイダセキュア
コンテナ供給処理スタート
セキュアコンテナの証明書から公開鍵を取り出す
S221
セキュアコンテナの改竄がないことを確認する
S222
セキュアコンテナからUCPを取り出す
S223
PTを作成
S204
セキュアコンテナを作成
S225
レシーバと相互認証する
S226
セキュアコンテナを送信
S227
リターン

図４５

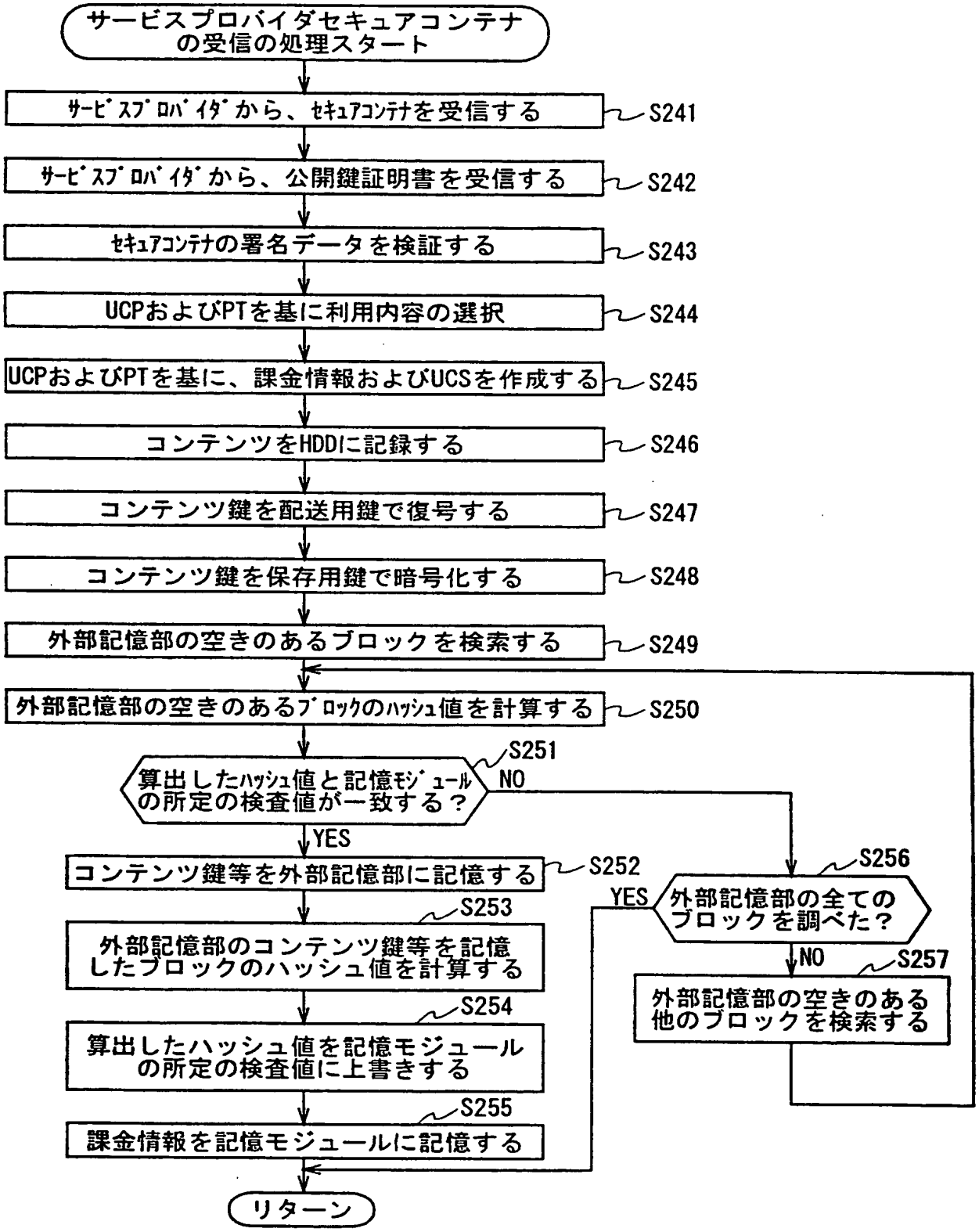

サービスプロバイダセキュアコンテナの受信の処理スタート
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞから、ｾｷｭｱｺﾝﾃﾅを受信する
S241
ｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞから、公開鍵証明書を受信する
S242
ｾｷｭｱｺﾝﾃﾅの署名データを検証する
S243
UCPおよびPTを基に利用内容の選択
S244
UCPおよびPTを基に、課金情報およびUCSを作成する
S245
コンテンツをHDDに記録する
S246
コンテンツ鍵を配送用鍵で復号する
S247
コンテンツ鍵を保存用鍵で暗号化する
S248
外部記憶部の空きのあるブロックを検索する
S249
外部記憶部の空きのあるﾌﾞﾛｯｸのﾊｯｼｭ値を計算する
S250
S251
算出したﾊｯｼｭ値と記憶ﾓｼﾞｭｰﾙの所定の検査値が一致する？
NO
YES
コンテンツ鍵等を外部記憶部に記憶する
S252
S253
外部記憶部のコンテンツ鍵等を記憶したブロックのハッシュ値を計算する
S254
算出したハッシュ値を記憶モジュールの所定の検査値に上書きする
S255
課金情報を記憶モジュールに記憶する
S256
YES
外部記憶部の全てのブロックを調べた？
NO
S257
外部記憶部の空きのある他のブロックを検索する
リターン

図４６

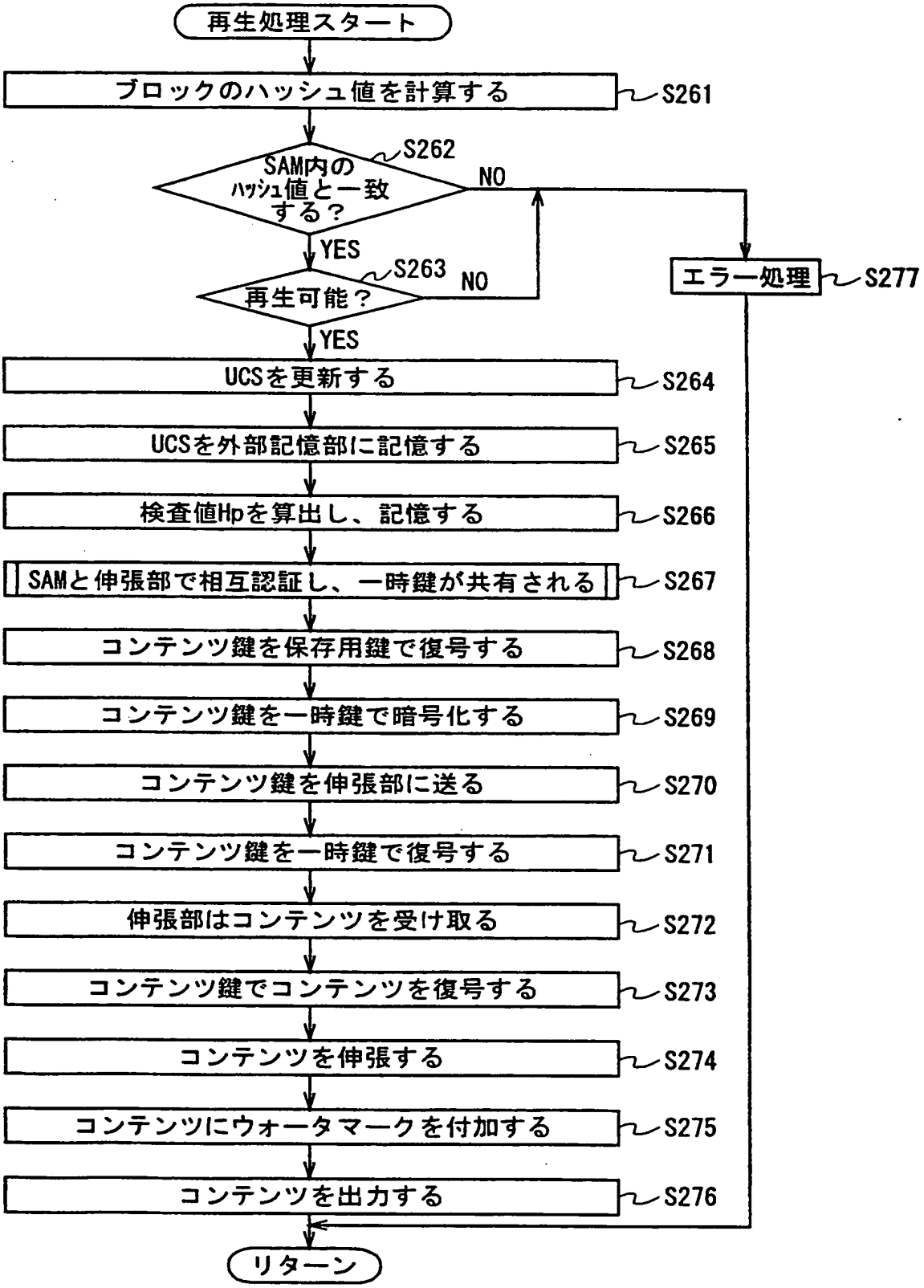

再生処理スタート
ブロックのハッシュ値を計算する
S261
SAM内のハッシュ値と一致する？
S262
NO
YES
再生可能？
S263
NO
エラー処理
S277
YES
UCSを更新する
S264
UCSを外部記憶部に記憶する
S265
検査値Hpを算出し、記憶する
S266
SAMと伸張部で相互認証し、一時鍵が共有される
S267
コンテンツ鍵を保存用鍵で復号する
S268
コンテンツ鍵を一時鍵で暗号化する
S269
コンテンツ鍵を伸張部に送る
S270
コンテンツ鍵を一時鍵で復号する
S271
伸張部はコンテンツを受け取る
S272
コンテンツ鍵でコンテンツを復号する
S273
コンテンツを伸張する
S274
コンテンツにウォータマークを付加する
S275
コンテンツを出力する
S276
リターン

図４７

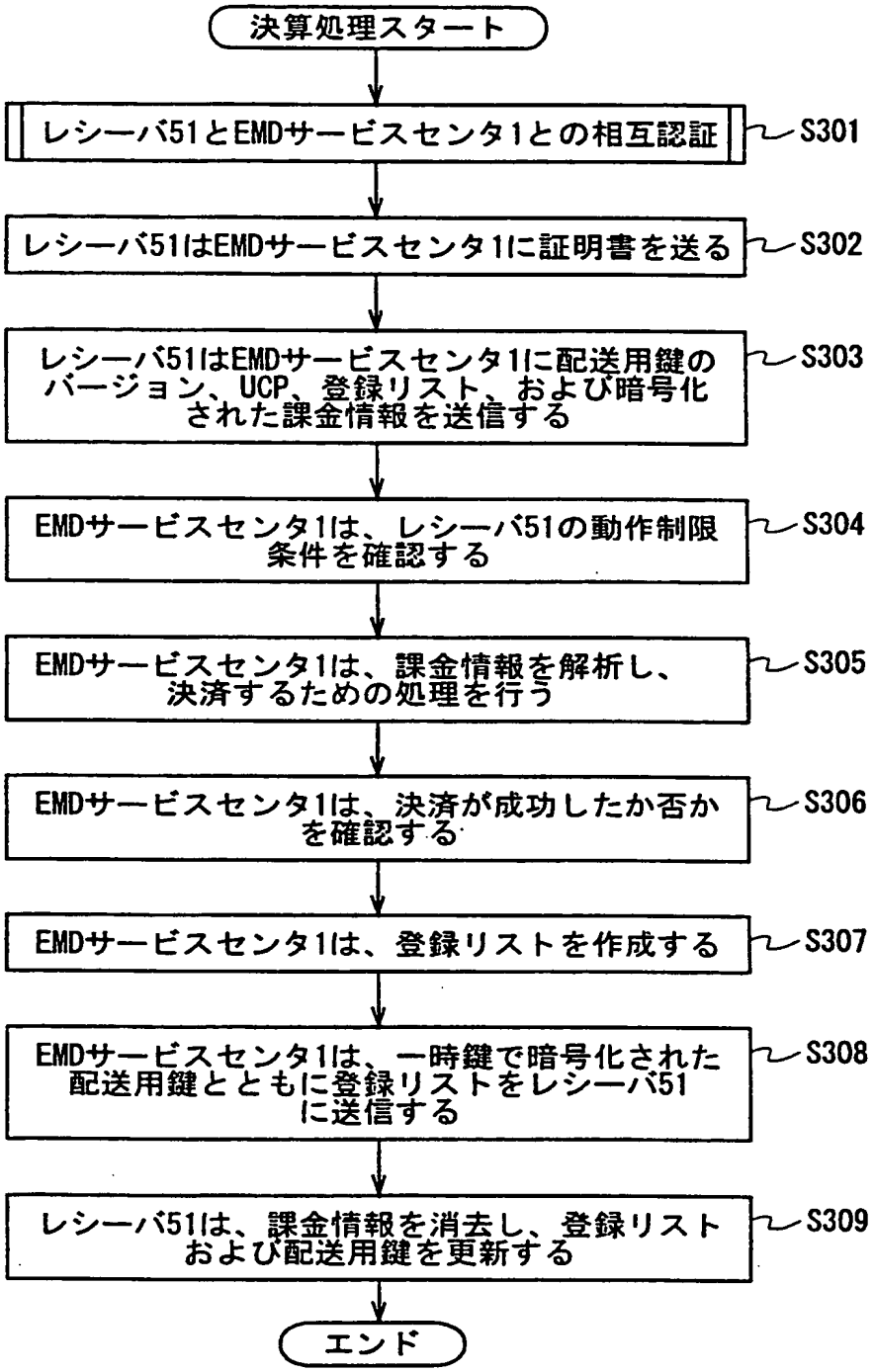

決算処理スタート
レシーバ51とEMDサービスセンタ1との相互認証
S301
レシーバ51はEMDサービスセンタ1に証明書を送る
S302
レシーバ51はEMDサービスセンタ1に配送用鍵のバージョン、UCP、登録リスト、および暗号化された課金情報を送信する
S303
EMDサービスセンタ1は、レシーバ51の動作制限条件を確認する
S304
EMDサービスセンタ1は、課金情報を解析し、決済するための処理を行う
S305
EMDサービスセンタ1は、決済が成功したか否かを確認する
S306
EMDサービスセンタ1は、登録リストを作成する
S307
EMDサービスセンタ1は、一時鍵で暗号化された配送用鍵とともに登録リストをレシーバ51に送信する
S308
レシーバ51は、課金情報を消去し、登録リストおよび配送用鍵を更新する
S309
エンド

図４８

符 号 の 説 明

1... EMDサービスセンタ，2... コンテンツプロバイダ，3... サービスプロバイダ，5... ユーザホームネットワーク，11... サービスプロバイダ管理部，12... コンテンツプロバイダ管理部，13... 著作権管理部，14... 鍵サーバ，15... 経歴データ管理部，16... 利益分配部，17... 相互認証部，18... ユーザ管理部，19... 課金請求部，20... 出納部，21... 監査部，31... コンテンツサーバ，32... ウォータマーク付加部，33... 圧縮部，34... 暗号化部，35... 乱数発生部，36... 暗号化部，37... ポリシー記憶部，38... セキュアコンテナ作成部，39... 相互認証部，41... コンテンツサーバ，42... 値付け部，43... ポリシー記憶部，44... セキュアコンテナ作成部，45... 相互認証部，51... レシーバ，52... HDD，61... 通信部，62... SAM，63... 外部記憶部，64... 伸張部，65... 信部，66... インタフェース，67... 表示制御部，68... 入力制御部，71... 相互認証モジュール，72... 課金処理モジュール，73... 記憶モジュール，74... 復号／暗号化モジュール，75... データ検査モジュール，91... 復号ユニット，92... 乱数発生ユニット，93... 暗号化ユニット，101... 相互認証モジュール，102... 復号モジュール，103... 復号モジュール，104... 伸張モジュール，105... ウォータマーク付加モジュール，201... レシーバ，202... HDD，211... 通信部，212... SAM，213... 外部記憶部，214... 伸張部，215... 通信部，216... インタフェース，217... 表示制御部，218... 入力制御部，221... 相互認証モジュール，222... 課金処理モジュール，223... 記憶モジュール，224... 復号／暗号化モジュール，225... データ検査モジュール，2

３１... 復号ユニット，２３２... 乱数発生ユニット，２３３... 暗号化ユニット，２４１... 相互認証モジュール，２４２... 復号モジュール，２４３... 復号モジュール，２４４... 伸張モジュール，２４５... ウォータマーク付加モジュール

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/02289

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F17/60, G06F13/00, G09C1/00, H04L9/08, G06F15/00, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-2000
Kokai Jitsuyo Shinan Koho 1971-2000 Toroku Jitsuyo Shinan Koho 1994-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST Data Base (JOIS)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO, 96/27155, A2 (InerTrust Technologies Corp.), 6 September, 1996 (06.09.96) &JP, 10-512074, A	1-9
A	US, 6002771, A (Sun Microsystems, Incorporated), 22 May, 1996 (22.05.96) & JP, 10-055383, A	1-9

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 May, 2000 (24.05.00)	13 June, 2000 (13.06.00)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

国際調査報告

国際出願番号　PCT／JP00／02289

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl' G06F17/60

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl' G06F17/60 G06F13/00 G09C1/00 H04L9/08 G06F15/00 H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報　1926-1996年
日本国公開実用新案公報　1971-2000年
日本国実用新案登録公報　1996-2000年
日本国登録実用新案公報　1994-2000年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

JICSTデータベース(JOIS)

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	WO,96/27155,A2(InerTrust Technologies Corp.),6.9月.1996(06.09.96&JP,10-512074,A	1-9
A	US,6002771,A(Sun Microsystems, Incorporated)22.5月.96(22.05.96)&JP,10-055383,A	1-9

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
24.05.00	13.06.00

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	岩間　直純	5L	9287
	電話番号　03－3581－1101　内線　3532		